UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

MICHAEL DALLUM and JEREMY PADOW, on Behalf of Themselves and All Others Similarly Situated,

Plaintiffs,

v.

KINO LORBER LLC,

Defendant.

Case No.: 1:24-cv-8775

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Michael Dallum and Jeremy Padow ("Plaintiffs"), individually and on behalf of all others similarly situated, by and through their undersigned counsel, bring this class action complaint against Defendant Kino Lorber LLC, formerly known as Kino International Corporation ("Kino Lorber" or "Defendant"), which owns and manages a film distribution website at https://kinolorber.com/ (the "Website"). On the Website, Defendant utilized tracking tools to intercept and disclose consumers' search terms, video watching information, and personally identifiable information without seeking or obtaining consumers' consent (the "Tracking Tools"). Defendant's use of the Tracking Tools resulted in violations of the Video Privacy Protection Act ("VPPA"), federal and state wiretap laws, and invasions into consumers' privacy. Plaintiffs allege the following upon information and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiffs, which are alleged upon personal knowledge.

NATURE OF THE ACTION

1. This is a class action brought on behalf of all persons who visited Defendant's Website and purchased pre-recorded video materials (the "Consumers").

2. Defendant has been distributing foreign language and domestic arthouse films for over 30 years. Defendant's offerings range from classic silent titles to contemporary films from around the world. Defendant handles more than 500 movies from 30 countries and in 23 different languages.

3. Consumers can purchase Defendant's pre-recorded video materials in the form of DVDs, Blu-rays, and 4k movies through the Website after providing their personal information to create a Kino Lorber account.

4. In short, the Defendant is in the business of selling and delivering DVD, Blu-ray, and 4k Home videos to Consumers.

5. In all instances, the searching and purchasing of Defendant's videos are monitored by third parties as a result of Defendant's decision to place the Tracking Tools on each individual page containing Defendant's video materials on the Website.

6. Defendant does not disclose that Consumers' sensitive information, including personal identifying information ("PII"),[1] would be captured by the Tracking Tools, and then transmitted to third parties.

7. The Website does not inform Consumers that their PII will be exposed, available, and readily usable by any person of ordinary technical skill who receives that data.

8. At no point during or after the account sign up process does Defendant seek or obtain consent for the sharing of Consumers' PII, search terms, or the precise location of each webpage visited by Consumers, which Defendant surreptitiously gathered through the use of the Tracking Tools that it chose to employ on the Website. Assuming Defendant's Terms had been

[1] 18 U.S.C. § 2710(a)(3) ("includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider").

presented to Consumers, the Terms still do not warn Consumers that their PII and search terms will be disclosed to third parties.

9. In today's data driven world, a company's data sharing policies for a service or subscription are important factors for individuals to consider in deciding whether to provide personal information to that service or commit to a subscription.

10. Congress has recognized the immediate and irreversible harm caused by associating and disclosing a person's personally identifiable information in conjunction with their video watching information.

11. Congress' enactment of the VPPA, and its continued endorsement of the statute, supports that recognition. The VPPA prohibits video tape service providers ("VTSP"),[2] such as Defendant, from sharing consumers' PII without valid consent.[3]

12. Congress made clear that the harm to individuals impacted by VPPA violations occurs the moment, and each time, a subscriber's information is shared.

13. On the Website, because of Kino Lorber's decision to employ Meta, Inc.'s ("Facebook" or "Meta") tracking pixel (the "Pixel," discussed and defined herein) and because it chose to employ the Pixel on its video content on the Website, a consumer's PII is shared *the moment* the consumer purchases video materials.[4]

---

[2] VTSP refers to "any person, engaged in the business . . . of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials . . . ." 18 U.S.C. § 2710(a)(4).
[3] 18 U.S.C. § 2710(b)(2)(B)(i)-(iii).
[4] As defined by the VPPA, protected "personally identifiable information" includes information which identifies a person as having "*requested* or obtained" video materials. *See* 18 U.S.C. § 2710(a)(3). When a website user clicks a link leading to a video, the user "requests" authorization to access the material from the website's server and, if authorized, the server then sends the data to the user. *See How the Web works*, MOZILLA https://developer.mozilla.org/en-US/docs/Learn/Getting_started_with_the_web/How_the_Web_works (last visited Nov. 15, 2024).

14. Defendant purposefully implemented and utilized the Pixel, which tracks consumers' activity on the Website and discloses that information to Facebook to gather valuable marketing data. The Pixel could not be placed on the Website without steps taken directly by or on behalf of Defendant (*see* Section B(1)(a)).

15. To be clear, the Pixel cannot be placed on a website by Facebook. Only a website owner can place the Pixel on a website. Here, the Pixel was utilized on the Kino Lorber Website, and effectuates the sharing of Consumers' PII. None of this could have occurred without purposeful action on the part of Defendant.

16. Defendant does not seek and has not obtained consent from Consumers to utilize the Pixel to track, share, and exchange their PII, search terms, and precise webpage information with Facebook.

17. When a party, such as Kino Lorber, utilizes the Pixel, it is provided with details about its functionality, including the collection and disclosure of its Consumers' PII.[5]

18. In fact, it is made aware that one of the functions of the Pixel is to collect and share PII to "use that information to provide measurement services[] [and] target and deliver ads."[6]

19. Facebook also advises and directs website owners that there are notice and consent requirements associated with the use of the Pixel in that website owners are responsible to provide that notice and obtain those consents.

[5] *Meta Business Tools Terms*, FACEBOOK, https://www.facebook.com/legal/terms/businesstools ("You represent and warrant that you have provided robust and sufficiently prominent notice to users regarding the Business Tool Data collection, sharing and usage . . . Meta[] may use cookies web beacons and other storage technologies to collect or receive information from your websites . . . .") (last visited Nov. 15, 2024).
[6] *Id.*

20. Not only did Kino Lorber know that Consumers' PII would be shared, it was on notice of its obligations to provide notice of its data gathering practices and obtain consent from Consumers.

21. Defendant cannot claim surprise as to the nature of the Pixel when Facebook itself warned websites utilizing the Pixel, aside from needing "a clear and prominent notice on each web page where [its] Pixels are used[,]" that they must "ensure, in a verifiable manner, that an end user provide[d] all necessary consents before [Kino Lorber] use[d] [Facebook's Pixel] to enable the storage of and access to Meta cookies . . . [i]n jurisdictions that require informed consent."[7] Employing the Pixel on the Website caused Consumers' PII to be shared with third parties, resulting in VPPA violations.

22. Defendant, despite its use of the Pixel on the pages of the Website selling pre-recorded video content, failed to obtain Consumers' consent to allow the Pixel to operate in a way that shares Consumers' protected information with Facebook.

23. Federal and state legislatures addressed citizens' privacy expectations when communicating with parties via electronic communications.

24. Congress passed the Federal Wiretap Act, which prohibits the unauthorized interception of electronic communications.

25. California passed the California Invasion of Privacy Act ("CIPA"), which attaches liability to any person who, willfully and without the consent of all parties to a communication, attempts to read or to learn the contents or meaning of any message or communication while it is

[7] *Id.*; *see infra* Section B(1)(d).

in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within California.[8]

26. Defendant purposefully implemented and utilized the Tracking Tools to intercept and read Consumers' PII and communications with the Website. Defendant knew that the Tracking Tools would feed Consumers' PII and communications to third parties. The Website does not provide notice of or obtain consent as to such practices.

27. Consumers of the Website have been harmed as a result of violations of the VPPA, the Federal Wiretap Act, and CIPA. In addition to monetary damages, Plaintiffs seek injunctive relief requiring Defendant to immediately (i) remove the Pixel from the Website, or (ii) add adequate notices and obtain the appropriate consent from subscribers.[9]

28. Finally, Plaintiffs had their privacy interests, enshrined under Article 1, Section 1 of California's Constitution, violated.

29. Consumers of the Website, such as Plaintiffs, have an interest in maintaining control over their private and sensitive information, such as their search terms, as well as an interest in preventing their misuse.

30. Plaintiffs' claims are brought as a class action, pursuant to Federal Rule of Civil Procedure 23, on behalf of themselves and all other similarly situated persons. Plaintiffs seek relief in this action individually and on behalf of subscribers of the Website for violations of the VPPA, 18 U.S.C. § 2710, violations of CIPA, Cal. Penal Code § 631 and § 635, violations of the

---

[8] Cal. Penal Code § 631(a).

[9] Website owners like Criterion also have the option to anonymize the video's title within the URL or encrypt the video title using hashing, as described by Facebook. *See Advanced Matching*, FACEBOOK https://developers.facebook.com/docs/meta-pixel/advanced/advanced-matching#security (last visited Nov. 15, 2024); *Meta Business Tools Terms*, FACEBOOK, https://www.facebook.com/legal/terms/businesstools ("When using a Meta image pixel or other Meta Business Tools, you or your service provider must hash [personally identifiable information] in a manner specified by us before transmission") (last visited Nov. 15, 2024).

Wiretap Act, 18 U.S.C. § 2511(1)(a)-(e), and for violating privacy rights as established by California's Constitution.

PARTIES

31. Plaintiff Michael Dallum is, and has been at all relevant times, a citizen of Utah who resides in Salt Lake City, Utah. Plaintiff Dallum became a purchaser of Kino Lorber by purchasing physical copies of pre-recorded video content, in the form of Blu-ray disks, from Defendant in or about December 2022. Plaintiff Dallum used the Website for its intended purposes to purchase video content available to Plaintiff Dallum through the Website. Plaintiff Dallum used a Chrome internet browser to purchase videos from Defendant's Website while logged into his Facebook account on the same browser. Plaintiff Dallum did not consent, agree, authorize, or otherwise permit Defendant to disclose his PII to Facebook. Plaintiff Dallum was not provided with written notice that Defendant discloses their consumers' PII, or any means of opting out of the disclosures of their PII. Still, Kino Lorber knowingly disclosed Plaintiff Dallum's PII to Facebook. During the course of Plaintiff Dallum's use of the Website, Defendant collected and shared his PII with Facebook each and every time one of the Pixel Events (discussed and defined herein) were triggered. If not for Defendant's use of the Tracking Tools, Plaintiff Dallum would continue his use of the Website. Plaintiff Dallum's Facebook profile includes his name, photos, friend list, and posts.

32. Plaintiff Jeremy Padow is, and has been at all relevant times, a citizen of California who resides in Chatsworth, California. Plaintiff Padow became a purchaser of Kino Lorber by purchasing physical copies of video content, in the form of Blu-ray disks, from Defendant in or about April 2024. Plaintiff Padow used the Website for its intended purposes to purchase physical video content available to Plaintiff Padow through the Website. Plaintiff Padow used a Chrome internet browser to purchase videos from Defendant's Website in the same browser Mr. Padow

used to access Facebook. Plaintiff Padow did not consent, agree, authorize, or otherwise permit Defendant to disclose his PII to Facebook. Plaintiff Padow was not provided with written notice that Defendant discloses their consumers' PII, or any means of opting out of the disclosures of their PII. Still, Kino Lorber knowingly disclosed Plaintiff Padow's PII to Facebook. During the course of Plaintiff Padow's use of the Website, Defendant collected and shared his PII with Facebook each and every time one of the Pixel Events (discussed and defined herein) were triggered. If not for Defendant's use of the Tracking Tools, Plaintiff Dallum would continue his use of the Website. Plaintiff Padow's Facebook profile includes his name, photos, workplace and work history, location, education history, and posts.

33. Defendant Kino Lorber LLC is a New York-based home-video distribution company that has a library of over 4,000 titles and is considered a leader in independent art house distribution, releasing 35 films per year theatrically. The company brings hundreds of titles annually to the home entertainment and educational markets through digital and physical media releases. Defendant is headquartered at Kino Lorber, Inc. 333 W. 39th St., Ste. 503, New York, NY 10018.

JURISDICTION AND VENUE

34. The District Court for the Southern District of New York has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class Members; the aggregate amount in controversy exceeds $5,000,000.00, exclusive of interest, fees, and costs; and at least one Class Member is a citizen of a state different from Defendant. This Court also has jurisdiction over this action pursuant to 28 U.S.C. § 1331 because it arises under the.

35. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is in New York, and Defendant derives revenue in the State of New York, including Defendant's revenue generated from its management over and sales through the

Website, including the revenue sharing, advertising sales, etc. that Defendant derives from the Website.

36. Venue is proper in the Southern District of New York pursuant to 28 U.S.C. § 1391 because Defendant's principal place of business is located in this District and Defendant conducts substantial business operations in this District. In connection with the Website, the video sales, and associated coding, all claims originate and arise out of the Defendant's business operations in this District.

COMMON FACTUAL ALLEGATIONS

A. Legislative Background

1. The Video Privacy Protection Act

37. "The Video Privacy Protection Act follows a long line of statutes passed by the congress to extend privacy protection to records that contain information about individuals." S. Rep. No. 100-599 at 2 (1988). Starting with the Fair Credit Reporting Act of 1970, Congress sought to protect the "confidentiality of personal information" and passed multiple laws that "expanded and [gave] meaning to the right of privacy." *Id.*

38. In 1977, Congress amended the Privacy Act, which mandated the creation of the Privacy Protection Study Commission ("the Commission"), which studied "'data banks, automated data processing programs, and information systems of governmental, regional, and private organizations, in order to determine the standards and procedures in force for the protection of personal information.'" *Id.* (quoting 95-38). The Commission concluded that an effective national information policy must: (i) minimize intrusiveness; (ii) maximize fairness; and (iii) create legitimate, enforceable expectations of confidentiality. *Id.* "As a general rule, the Commission recommended that organizations which maintained a confidential records system be

placed under a legal duty not to disclose the record without the consent of the individual, except in certain limited circumstances. . . ." *Id.* at 2-3.

39. In 1988, Congress was again forced to act when a Washington-based newspaper published a profile of Judge Robert H. Bork "based on the titles of 146 films his family had rented from a video store." *Id.* at 5. Senators took to the floor to denounce the act, with Senator Patrick Leahy noting that:

40. In an era of interactive television cables, the growth of computer checking and check-out counters . . . all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch . . . I think it is something that we have to guard against.

Id. at 5-6.

41. Congress believed that these "information pools" created privacy interests that directly affected the ability of people to freely express their opinions, join in association with others, or enjoy the general freedoms and independence protected by the Constitution. *Id.* at 7.

42. As Senator Patrick Leahy and the late Senator Paul Simon recognized, records of this nature offer "a window into our loves, likes, and dislikes," such that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance." *Id.* at 7-8 (statements of Sens. Simon and Leahy, respectively).

43. Senator Simon lamented that "[e]very day Americans are forced to provide to businesses and others personal information without having any control over where that information goes." *Id.* at 6-7.

44. As a result, Senate Bill 2361 was drafted to "give meaning to, and thus enhance, the concept of privacy for individuals in their daily lives" by prohibiting "unauthorized disclosures of personal information held by video tape providers." *Id.* at 6.

45. When contemplating the VPPA, Congress noted Supreme Court precedent recognizing a privacy right in the lists that reveal personal beliefs and an individual's choice of books and films. *Id.* at 4.

46. The VPPA regulates the disclosure of information about consumers' consumption of video content, imposing specific requirements to obtain consumers' consent to such disclosure. Under the statute, for each violation of the statute, a court may award actual damages (but not less than liquidated damages of $2,500.00 per person), punitive damages, equitable relief, and attorney's fees.

47. The statutory damages were deemed "necessary to remedy the intangible harm caused by privacy intrusions." *Id.* at 8.

48. The VPPA prohibits "[a] video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider." 18 U.S.C. § 2710(b)(1).

49. Consumer is defined as "any renter, purchaser, or subscriber of goods or services from a video tape service provider[.]" 18 U.S.C. § 2710(a)(1). The plain language of the definition of consumer appears first among the subsections of the VPPA, and uses broad language to define what a consumer is.

50. The VPPA defines personally identifiable information as "information which identifies a person as having requested or obtained specific video materials or services from a video service provider." 18 U.S.C. § 2710(a)(3). Here, Congress made special note that:

51. The definition of personally identifiable information includes the term "video" to make clear that simply because a business is engaged in the sale or rental of video materials or services does not mean that all of its products or services are within the scope of the bill. For example, a department store that sells video tapes would be required to extend privacy protection to only those transactions involving the purchase of video tapes and not other products. This definition makes clear that personally identifiable information is intended to be transaction-oriented. It is information that identifies a particular person as having engaged in a specific transaction with a video tape service provider. The bill does not restrict the disclosure of information other than personally identifiable information.

52. Senate Report 100-599, at 12 (1988) (emphasis added).

53. Congress wanted to ensure that any transaction between consumer and VTSP involving a request or procurement of specific video materials or video services would be protected. In short, the language is broad enough to encompass digital as well as physical transactions, so long as the transaction includes the defined and prohibited information.

54. A VTSP is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710(a)(4).

55. While 18 U.S.C. § 2710(a)(3) limits PII to information identifying a person as having requested "specific video materials or services" and 18 U.S.C. § 2710(a)(4) limits VTSP to a person in the business of renting, selling, or delivering prerecorded audio visual materials, affected consumers are not limited by any such link to "video *materials*" or "audio visual *materials."* Instead, consumer applies to "*goods* or services" from a VTSP generally.[10]

[10] *See Salazar v. Nat'l Basketball Ass'n*, slip op., No. 23-1147 (2d Cir. Oct. 15, 2024).

56. The wide scope of consumer comports with the initial purpose of the VPPA, which was initially passed in 1988 for the purpose of protecting the privacy of individuals' video rental, purchase, and viewing data.

57. In 2012, Congress amended the VPPA, and in so doing, reiterated the Act's applicability to "so-called 'on-demand' cable services and Internet streaming services [that] allow consumers to watch movies or TV shows on televisions, laptop computers, and cell phones." S. Rep. 112-258, at 2.

58. During a recent Senate Judiciary Committee meeting, "The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century," Senator Leahy stated that "[w]hile it is true that technology has changed over the years, we must stay faithful to our fundamental right to privacy and freedom. Today, social networking, video streaming, the 'cloud,' mobile apps and other new technologies have revolutionized the availability of Americans' information."[11]

59. This application of the VPPA to modern video sources, such as websites, has been confirmed by various courts across the country.[12]

60. Defendant here is a video service provider as it provided pre-recorded audio-visual materials to Plaintiffs and Class Members on their Website.

61. The relationship between Plaintiffs and Defendant is precisely the type of relationship contemplated by the VPPA.

---

[11] See *Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law, The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century*, SENATE JUDICIARY COMMITTEE SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW, *available at* https://www.judiciary.senate.gov/download/hearing-transcript_-the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21st-century (last visited Nov. 15, 2024).

[12] *See, e.g., Sellers v. Bleacher Report, Inc.,* 2023 U.S. Dist. LEXIS 131579, at *15-18 (N.D. Cal. July 29, 2023) (VPPA sufficiently applied to sports news website); *Jackson v. Fandom, Inc.,* 2023 U.S. Dist. LEXIS 125531, at *6 (N.D. Cal. July 20, 2023) (VPPA applies to gaming and entertainment website); *Louth v. NFL*, 2022 U.S. Dist. LEXIS 163706, at *11-12 (D.R.I. Sep. 12, 2022) (holding VPPA applied to NFL's videos accessible through mobile app).

62. In this case, Plaintiffs' PII was knowingly and systematically disclosed to Facebook, without obtaining their consent.

2. The Federal Wiretap Act

63. The Federal Wiretap Act (the "Wiretap Act") was enacted in 1934 "as a response to Fourth Amendment concerns surrounding the unbridled practice of wiretapping to monitor telephonic communications."[13]

64. The Wiretap Act primarily concerned the government's use of wiretaps but Congress grew concerned that technological advancements like "large-scale mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing" were rendering the Wiretap Act out of date.[14] Thus, in 1986, Congress amended the Wiretap Act through the Electronic Communications Privacy Act ("ECPA") to provide a private right of action for private intrusions as though they were government intrusions.[15]

65. The ECPA primarily focused on two types of computer services that were prominent in the 1980s: (i) electronic communications like email between users; and (ii) remote computing services like cloud storage or third party processing of data and files.[16]

66. Title I of the ECPA amended the Wiretap Act such that a violation occurs when a person or entity: (i) provides an electronic communication service to the public; and (ii)

---

[13] Hayden Driscoll, *Wiretapping the Internet: Analyzing the Application of the Federal Wiretap Act's Party Exception Online*, 29 WASH. & LEE J. C.R. & SOC. JUST. 187, 192 (2022), https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=1541&context=crsj (last visited November 18, 2024).

[14] Senate Rep. No. 99-541, at 2 (1986).

[15] Hayden Driscoll, *Wiretapping the Internet: Analyzing the Application of the Federal Wiretap Act's Party Exception Online*, 29 WASH. & LEE J. C.R. & SOC. JUST. 187, 192 (2022), https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=1541&context=crsj (last visited November 18, 2024).

[16] *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1103 (9th Cir. 2014).

intentionally divulges the contents of any communication; (iii) while the communication is being transmitted on that service; (iv) to any person or entity other than the intended recipient of such communication.

67. While the ECPA allows a single party to consent to the interception of an electronic communication, single party consent is only acceptable where the communication is not "intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. §2511(2)(d).

68. While communicating with Defendant on the Website through their viewing choices, Consumers had the contents[17] of their communications with Defendant intercepted by third parties via the Tracking Tools.

69. Defendant purposefully included the Tracking Tools on the Website to intercept Plaintiffs' communications and redirect them to third parties to improve the effectiveness of its and the third parties' advertising and marketing.

70. Plaintiffs did not know of or consent to the exposure of their legally protected communications with Defendant to third parties.

[17] The contents of Plaintiffs' and users' communications include: 1) search terms submitted to the site; 2) the location and contents of webpages visited by users; and 3) the PII discussed in Section B.

3. The California Invasion of Privacy Act

71. CIPA was enacted in 1967 for the expressly stated purpose "to protect the right of privacy of the people of [California]."[18] The California legislators were concerned about emergent technologies that allowed for the "eavesdropping upon private communications," believing such technologies "created a serious threat to the free exercise of personal liabilities and cannot be tolerated in a free and civilized society."[19]

72. CIPA is regularly recognized as California's analog to the Federal Wiretap Act, comprised of the same general elements and protect against the same general harms.

73. To protect people's privacy, legislators broadly protected wired and aural communications being sent to or received from California.[20] Notably, for wired communications, California set out to prohibit (i) intentional wiretapping or (ii) willful attempts to learn the contents of wired communications, (iii) attempts to use or transmit information obtained through wiretapping, or (vi) aiding, agreeing with, employing, or conspiring with any person(s) to unlawfully do, permit, or cause the preceding three wrongs.[21]

74. CIPA also prohibits the manufacture, assembly, sale, offer for sale, advertisement for sale, possession, or furnishment to another of devices which are primarily or exclusively designed or intended for eavesdropping upon the communication of another.[22]

75. CIPA claims are often treated as analogous to Wiretap Act claims.

---

[18] Cal. Penal Code § 630.
[19] *Id.*
[20] Cal. Penal Code § 631-32.
[21] *Mastel v. Miniclip SA*, 549 F. Supp. 3d 1129, 1134 (E.D. Cal. 2021) (citing *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192 (1978)).
[22] Cal. Penal Code § 635.

B. The Website and the Tracking Tools

76. On the Website, Defendant utilized Tracking Tools created by Facebook, Google, Bing, The Trade Desk, and markhor.organicfruitapps.com (collectively, the "Tracking Entities") to intercept and disclose Consumers' search terms and PII without seeking or obtaining Consumers' consent.

1. The Website and the Facebook Pixel

77. Facebook offers the Pixel to web developers for the purpose of monitoring user interactions on their websites, which can then be shared with Facebook.

78. The Pixel is a marketing tool that can only be added to a webpage by website developers. A website operator must sign up for a business account or link a related Facebook account with its Pixel, and then add code to the website to make use of the Pixel.[23]

79. As Facebook notes, the Pixel must be added to each individual page that a website owner wishes to be tracked.[24]

80. Here, Defendant took steps to add the Pixel to the Website.

81. The Pixel is employed by Defendant to gather, collect, and then share user information with Facebook.[25] Receiving this information enables Facebook and the web developers to build valuable personal profiles for users, enhancing marketing effectiveness and increasing the chance of converting users into paying customers.[26] The sharing of Consumers' PII benefits Defendant by improving the effectiveness of advertising targeted at Defendant's

---

[23] *Meta Business Help Center: Set up and install the Meta Pixel*, FACEBOOK, https://www.facebook.com/business/help/952192354843755?id=1205376682832142 (last visited on Nov. 15, 2024).
[24] *Get Started*, FACEBOOK, https://developers.facebook.com/docs/meta-pixel/get-started/ ("To install the Pixel, . . . add its base code . . . on every page where you will be tracking website visitor actions") (last visited on Nov. 15, 2024).
[25] The Facebook Pixel allows websites to track visitor activity by monitoring user actions ("events") that websites want tracked and share a tracked user's data with Facebook. *See Meta Pixel*, FACEBOOK, https://developers.facebook.com/docs/meta-pixel/ (last visited on Nov. 15, 2024).
[26] *See Meta Pixel*, META, https://www.facebook.com/business/tools/meta-pixel (last visited on Nov. 15, 2024).

Consumers. Studies have shown that personalization in digital marketing through targeted and dynamic advertising can boost revenue by 15%.[27]

82. Website owners and operators can choose to use the Pixel to share both user activity (including video watching activity) and user identity with Facebook. Here, Defendant's Website shares both.

83. The harvested data can improve advertising by pinpointing audience demographics by interests, gender, or location and finding the people who are most likely to take action and view content.[28]

84. The PII harvested by Defendant provides similar, if not more, data, including the titles of videos, whether through search terms, webpage URLs, parameters, or metadata, in addition to their Facebook profile data.

85. The owner or operator of a website holds the decision-making authority over the placement of the Pixel on its site, as well as whether or not any of the data within the Pixel transmission should be "hashed" (a form of encryption).

2. Defendant Implemented the Pixel on the Website

86. To activate and employ a Facebook Pixel, a website owner must first sign up for a Facebook account, where adding the Pixel to the website owner's "business portfolio" provides the most utility for using the Pixel.[29] For instance, business portfolios can: (i) create and utilize more simultaneous Pixels, (ii) manage multiple Facebook Pages, Instagram accounts, ad

[27] Wilson Lau, *What is Targeted Advertising?*, ADROLL BLOG (June 30, 2024), https://www.adroll.com/blog/what-is-targeted-advertising#:~:text=Benefits%20of%20Targeted%20Advertising,-1.%20Deliver%20a%20higher (last visited Nov. 15, 2024).
[28] *See Meta Ads: Audience ad targeting*, FACEBOOK, https://www.facebook.com/business/ads/ad-targeting (last visited Nov. 15, 2024).
[29] *Meta Business Help Center: How to set up your Meta Pixel with a business portfolio*, META, https://www.facebook.com/business/help/314143995668266?id=1205376682832142 (last visited Nov. 15, 2024).

accounts, and catalogs from a centralized interface, (iii) access and manage multiple parties (which can then be given specific levels of access, including more easily revoking access to ex-employees), (iv) post or analyze data analytics collected from Facebook pages or Instagram accounts, (v) run ads businesses across Facebook and Instagram, and (v) create and manage shops across Facebook and Instagram.[30]

87. To add an operational Pixel to a website, the website owner or operator must take several affirmative steps, including naming the Pixel during the creation and setup of the Pixel.[31]

88. Once the Pixel is created, the website operator assigns access to the Pixel to specific people for management purposes,[32] and must connect the Pixel to a Facebook Ad account.[33]

89. After following these steps, a website operator can start capturing and sharing information using the Pixel.

90. A Pixel cannot be placed on a website by a third-party. It must be placed directly by or on behalf of the site owner.

91. Once the Pixel is set and activated, it can begin collecting and sharing user activity data as instructed by the website owner.

---

[30] *Meta Business Help Center: About business portfolios*, FACEBOOK, https://www.facebook.com/business/help/486932075688253 (last visited Nov. 15, 2024).

[31] *Id.; see also* Ivan Mana, *How to Set Up & Install the Facebook Pixel (In 2022)*, YOUTUBE, https://www.youtube.com/watch?v=ynTNs5FAUm8 (last visited Nov. 15, 2024).

[32] *Meta Business Help Center: Add People to Your Meta Pixel in Your Meta Business Suite or Business Manager*, FACEBOOK, https://www.facebook.com/business/help/279059996069252?id=2042840805783715 (last visited on Nov. 15, 2024).

[33] *Meta Business Help Center: Add an ad account to a Meta Pixel in Meta Business Manager*, FACEBOOK, https://www.facebook.com/business/help/622772416185967 (last visited on Nov. 15, 2024).

92. When a Facebook user logs onto Facebook, a "c_user" cookie – which contains a user's non-encrypted Facebook User ID number ("UID") – is automatically created and stored on the user's device for up to a year.[34]

93. This means that for Consumers to the Website who are also Facebook users, their PII is certain to be shared. Their PII is automatically bundled with their web watching history and disclosed to Facebook when visiting a page with an active Pixel, including the home page.

94. While the process to determine what information is being collected by the Pixel from a user is admittedly complicated, the recipient of the Pixel's transmissions receives the information in a clear and easy to understand manner.

95. The seemingly complex data, such as the long URLs included in the Pixel's transmission, is "parsed," or translated into an easier to read format, such that the information is legible.

96. For example, an embedded URL in a Pixel HTTP Request may look like an indecipherable code, as depicted below:

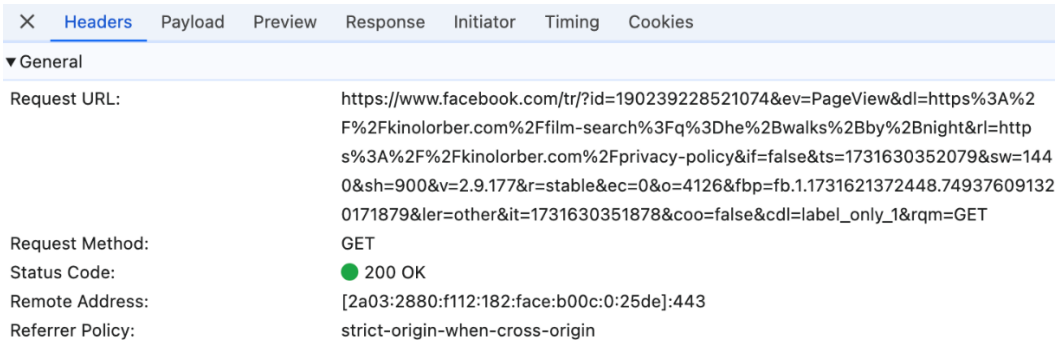


Figure 1 - Sample search on the Website using search terms "He Walked By Night"

97. However, these URLs are designed to be "parsed" into easy-to-digest pieces of information, as depicted below:

[34] *Cookie Policy: What are cookies and what does this policy cover?*, FACEBOOK, https://www.facebook.com/policy/cookies/ (last visited on Nov. 15, 2024).

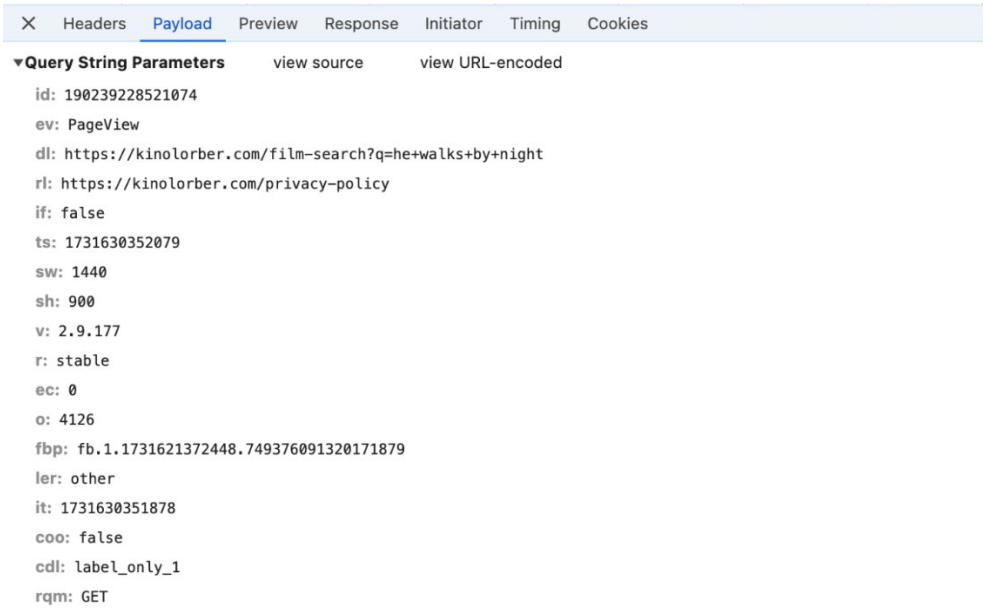


Figure 2 - Parsed URL Information from Sample Pixel Request

98. Similarly, the cookies attached to the Pixel's transmissions are parsed, as depicted below:

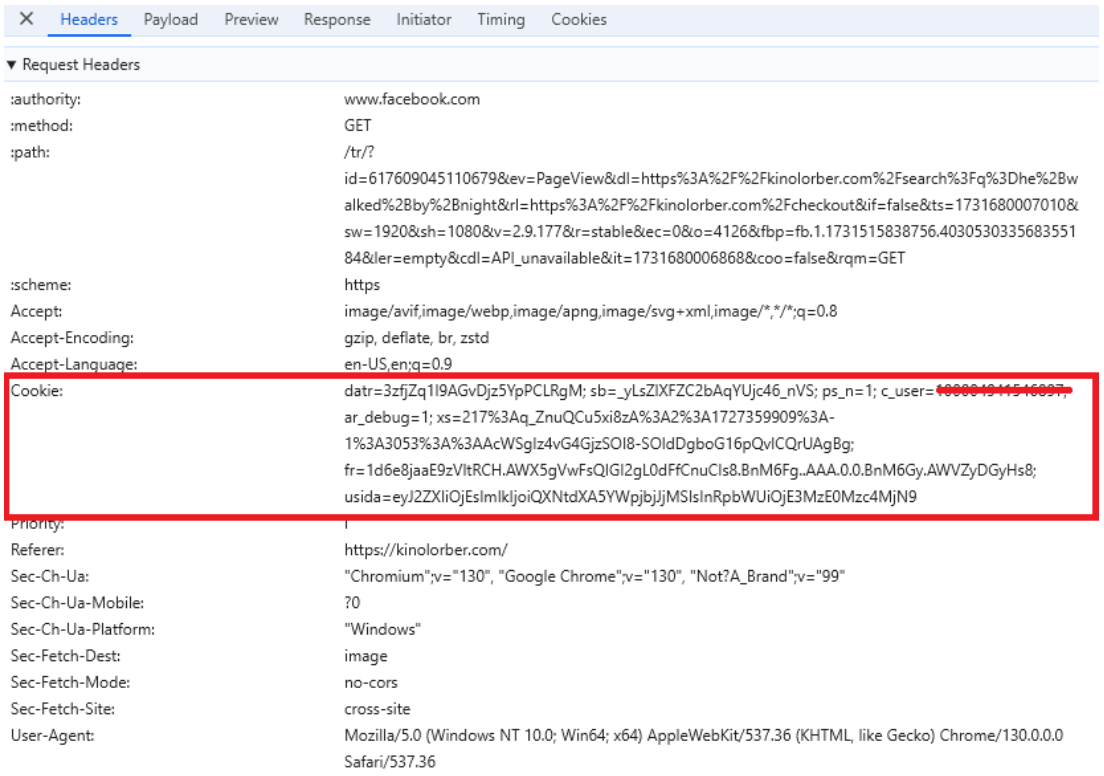


Figure 3- Cookie Data from Sample Pixel Request

99. PII can be used by anyone who receives the Pixel transmission to easily identify a Facebook user.

100. A UID is personally identifiable information. It contains a series of numbers used to identify a specific profile, as depicted below:

Figure 4 4 - Sample UID number of test account created by Plaintiffs' counsel in a prior investigation into the Pixel, captured by a Pixel event

101. The information contained within the c_user cookie is considered PII. It contains "the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching behavior."[35] Because the Facebook ID number can simply and easily be appended to "www.facebook.com/" to navigate to the relevant user's profile, it requires no special skill or expertise to identify the user associated with the Facebook ID, and courts have regularly upheld its status as PII.[36]

102. Any person, even without in-depth technical expertise, can utilize the UID to identify owners of the UID via their Facebook profile. Once the Pixel's routine exchange of information is complete, the UID that becomes available can be used by any individual of ordinary skill and technical proficiency to easily identify a Facebook user, by simply appending the Facebook UID to www.facebook.com (e.g., www.facebook.com/[UID_here]). That step, readily available through any internet browser, will direct the browser to the profile page, and all the information contained in or associated with the profile page, for the user associated with the

[35] *In re Nickelodeon Consumer Privacy Litigation,* 827 F.3d 262, 290 (3d Cir. 2016).
[36] *See Lebakken v. WebMD, LLC* 2022 U.S. Dist. LEXIS 201010, at *11-12 (N.D. Ga. Nov. 4, 2022); *Czarnionka v. Epoch Times Ass'n*, 2022 U.S. Dist. LEXIS 209067, at *8-10 (S.D.N.Y. Nov. 17, 2022); *Ambrose v. Boston Globe Media Partners, LLC*, 2022 U.S. Dist. LEXIS 168403, at *5-6 (D. Mass. Sept. 19, 2022).

particular UID. Using the UID from *Figure 5*, appending it to the Facebook URL in a standard internet browser (here, www.facebook.com/100091959850832) will redirect the webpage straight to the Facebook profile associated with the UID, as depicted below:

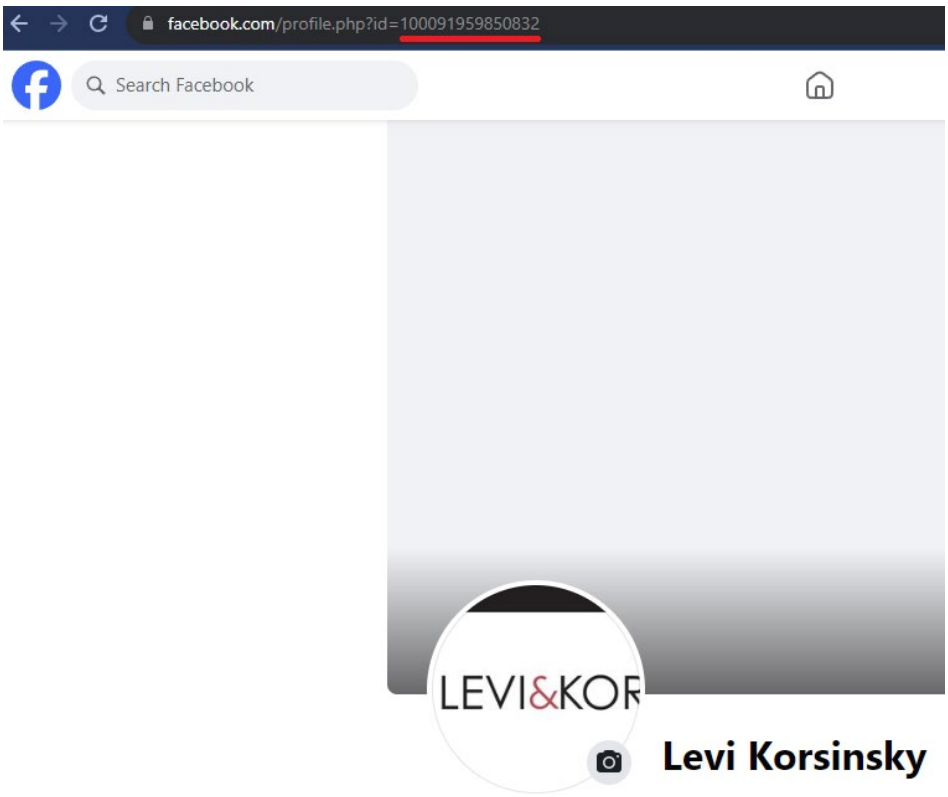


Figure 5 - Sample result of appending UID of a user to "facebook.com/" being redirected to the user's profile created by Plaintiffs' counsel in a prior investigation into the Pixel

103. Importantly, some Facebook profile information – name, gender, profile photo, cover photo, username, user ID (account number), age range, language, and country – are "always public."[37] No privacy setting on Facebook would allow Plaintiffs, or any user, to hide this basic information.

[37] *Control who can see what you share on Facebook*, FACEBOOK, https://www.facebook.com/help/1297502253597210 (last visited Nov. 15, 2024).

104. By compelling a user's browser to disclose the c_user cookie alongside event data for media content, Defendant knowingly discloses information sufficiently permitting an ordinary person to identify an individual.

a. The Pixel Shares Consumers' PII

105. The Pixel tracks user-activity on web pages by monitoring events,[38] which when triggered, causes the Pixel to automatically send data – here, Consumers' PII – directly to Facebook.[39] Examples of events utilized by websites include: (i) a user loading a page with a Pixel installed (the "PageView event") [40] and (ii) when pre-designated buttons, like the "Add to Cart" button, are clicked (the "SubscribedButtonClick" event) (collectively with the PageView event, the "Pixel Events").[41] The Website utilizes both.[42]

106. When the Pixel Events are triggered, a "HTTP Request" is sent to Facebook (through Facebook's URL www.facebook.com/tr/).[43] This confirms that the Pixel Events sent data to Facebook. The HTTP Request includes a Request URL and embedded cookies such as the c_user cookie. It may also include information in its Payload,[44] such as metadata tags. A Request URL, in addition to a domain name and path, contains parameters. Parameters are values added

---

[38] *Meta Business Help Center: About Meta Pixel*, FACEBOOK, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Nov. 15, 2024).
[39] *See generally id.*
[40] *Meta Business Help Center: Specifications for Meta Pixel standard events*, FACEBOOK, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited Nov. 15, 2024).
[41] *Reference: Standard Events*, FACEBOOK, https://developers.facebook.com/docs/meta-pixel/reference/ (last visited Nov. 15, 2024).
[42] The presence of Pixel events, such as the Microdata and PageView events, can be confirmed by using the publicly available and free Meta Pixel Helper tool. *See Meta Business Help Center: About the Meta Pixel Helper*, FACEBOOK, https://www.facebook.com/business/help/198406697184603?id=1205376682832142 (last visited Nov. 15, 2024).
[43] *How We Built a Meta Pixel Inspector*, THE MARKUP (Apr. 28, 2022) https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector.
[44] The "request payload" (or more simply, "Payload") is data sent by a HTTP Request, normally through a POST or PUT request, where the HTTP Request has a distinct message body. Payloads typically transmit form data, image data, and programming data. *See Request Payload Variation,* SITESPECT https://doc.sitespect.com/knowledge/request-payload-trigger (last visited Nov. 15, 2024).

to a URL to transmit data and direct a web server to provide additional context-sensitive services, as depicted below:

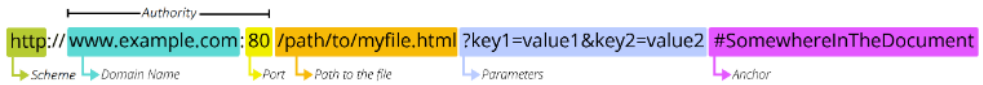


Figure 6 – Mozilla's diagram of a URL, including parameters[45]

107. Defendant uses the Pixel as a tracking method to collect and share Website Consumers' PII with Facebook. Defendant does not disclose its data sharing practices or obtain permission from its subscribers to share their PII with Facebook.

108. Defendant shares non-anonymized PII with Facebook. Defendant's disclosures include unique identifiers (the UID) that correspond to specific Facebook users. The recipient finds the PII and web watching history packaged together in a single data transmission which is easily readable by an ordinary person once the PII is packaged and delivered by the Website's Pixel.

109. Defendant monetizes the Website's Consumers by gathering Consumers' marketing data and PII and disclosing that valuable information to Facebook. Defendant does so in a format which allows it to make a direct connection between the identity of a Consumer and that Consumer's PII, without the consent of its Consumers and to the detriment of Plaintiffs' and Class Members' legally protected privacy rights.

110. Defendant had and continues to have the choice to design the Website so that the webpage URLs did not include the titles of videos. Defendant had, and has, the choice as to whether to purposefully include more information in the Website's URLs, including to improve website interaction and search engine optimization.[46] Here, Defendant chose to expose

[45] *What is a URL?*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL (last visited Nov. 15, 2024).
[46] *See* Chima Mmeje, *Different Domain Types and Best Practices for SEO,* MOZ (Nov. 11, 2024) https://moz.com/learn/seo/domain.

Consumers' video information so that it could benefit from the tracking and sharing of Consumers' PII.

111. Defendant also had the power to implement the Pixel in a way that shielded Consumers' sensitive information. Defendant chose, however, to transmit Consumers' non-anonymized PII.[47]

112. These factual allegations are corroborated by publicly available evidence. For instance, a user visits the Kino Lorber Website, clicks on a film, such as "He Walked By Night," and subsequently purchases the film.

113. Sensitive data sent to Facebook through the triggered Pixel Events are included within the parameters of the Request URL, within the Request Header, or as a Payload within the request. The specific Pixel Events implemented by Defendant sends Consumers' PII through the Request URL parameters and HTTP Headers.[48]

114. An "HTTP Header" is a field of an HTTP Request or response that passes additional context and metadata about the request or response.[49] Specifically, Request Headers are a subset of HTTP Headers that are used to provide information about a request's context, so that a server can customize its response to the request or supply authentication credentials[50] to the server or otherwise provide more information about the client sending the request.[51]

115. Defendant shares with Facebook the specific films requested and purchased by

---

[47] *See Advanced Matching*, FACEBOOK, https://developers.facebook.com/docs/meta-pixel/advanced/advanced-matching (last visited Nov. 15, 2024).
[48] URL parameters are values that are added to a URL to cause a web server to provide additional or different services. *What is a URL?,* MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL (last visited Nov. 15, 2024).
[49] *HTTP header*, MOZILLA, https://developer.mozilla.org/en-US/docs/Glossary/HTTP_header (last visited Nov. 15, 2024).
[50] *Id.*
[51] *Id.*

Consumers to the Website through Request URL parameters. This is portrayed in *Figures 8* through *10* below.

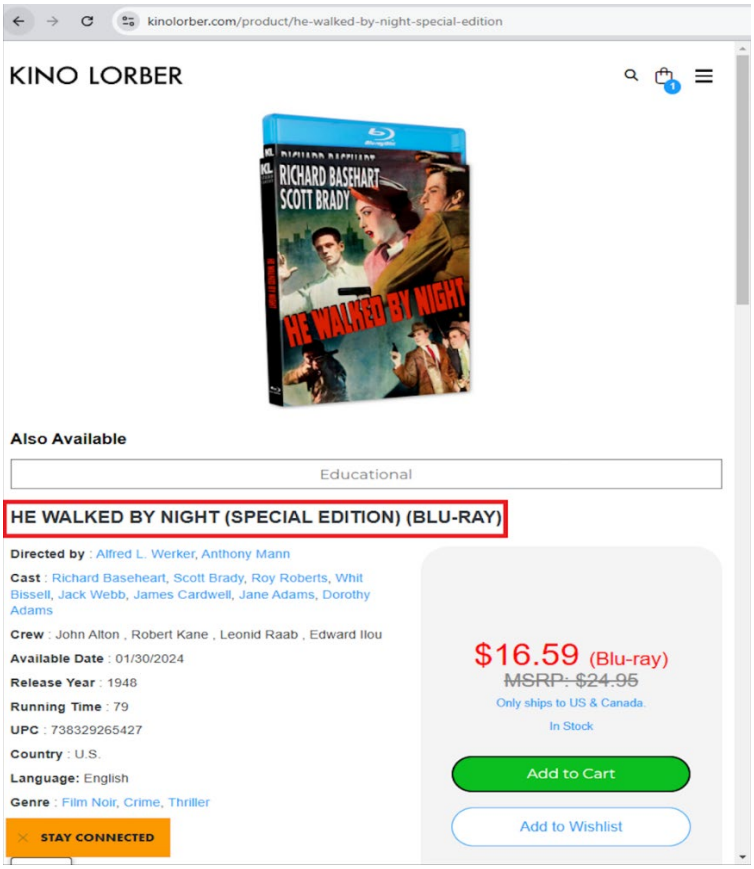


Figure 7 – Sample film webpage on the Website

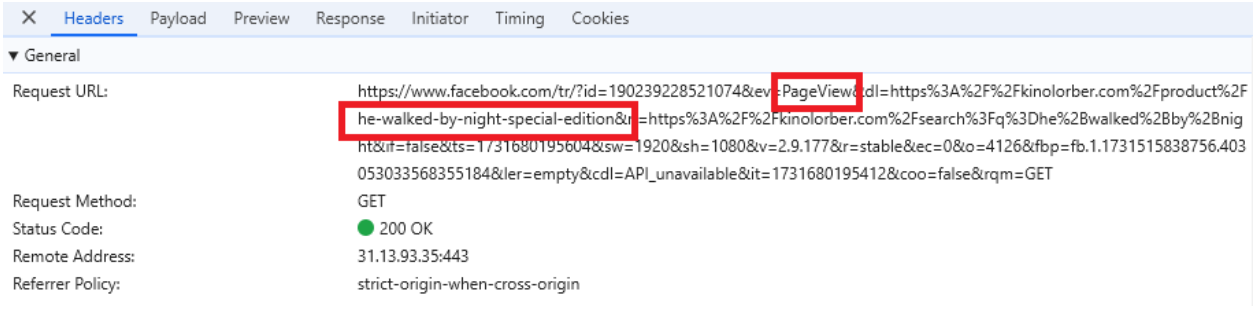
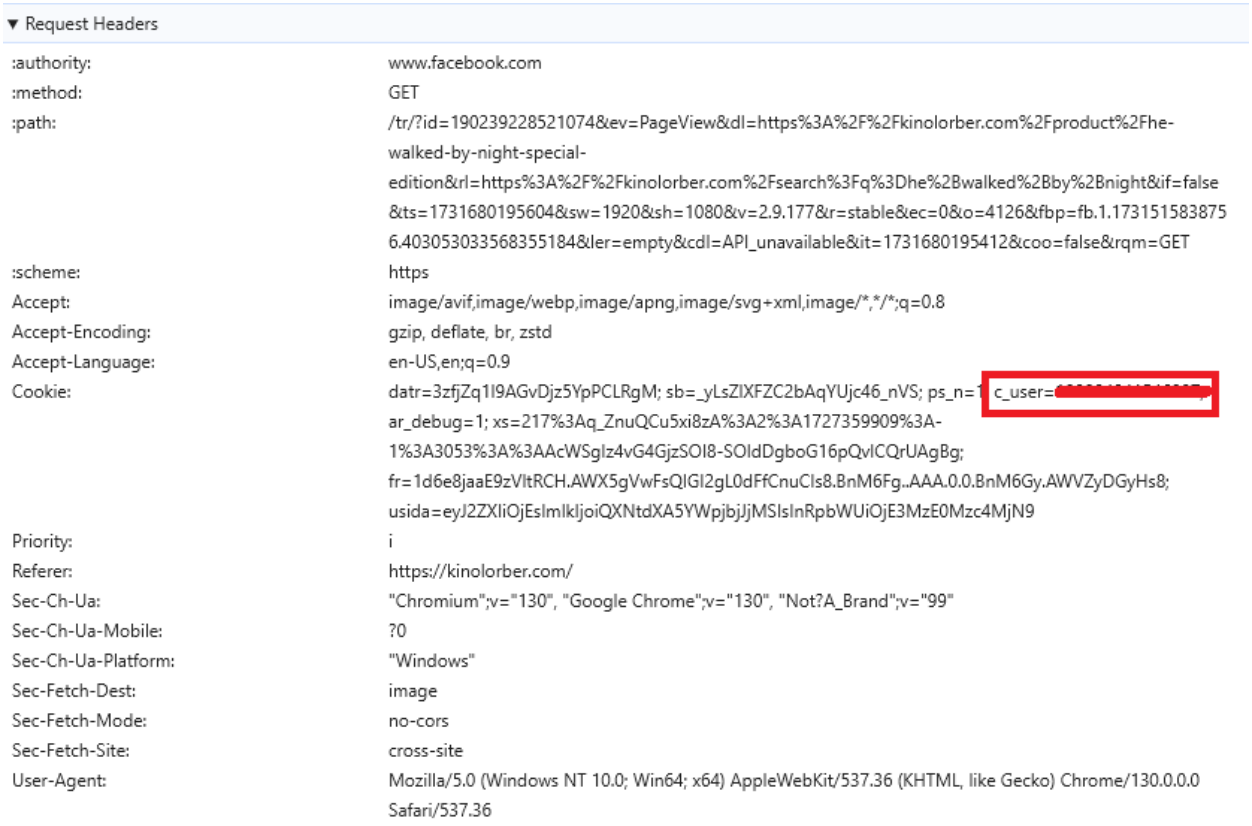


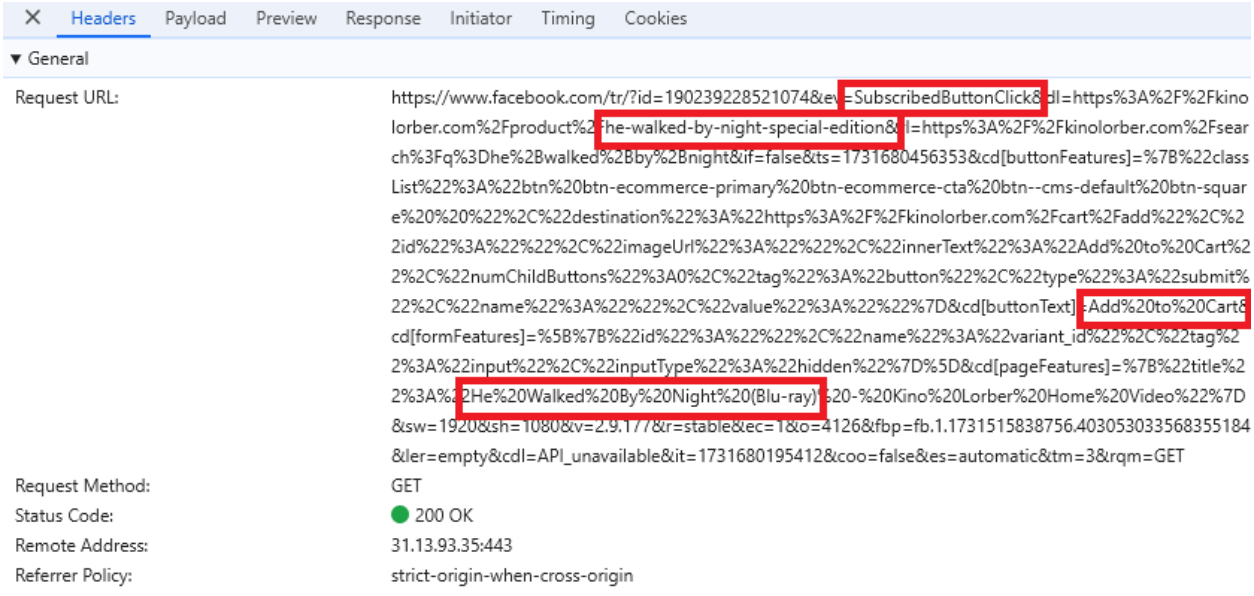
Figure 8 – Video Title included in URL parameters disclosed to Facebook through PageView Pixel Event on the Website



▼ Request Headers

:authority:	www.facebook.com
:method:	GET
:path:	/tr/?id=1902392285210 74&ev=PageView&dl=https%3A%2F%2Fkinolorber.com%2Fproduct%2Fhe-walked-by-night-special-edition&rl=https%3A%2F%2Fkinolorber.com%2Fsearch%3Fq%3Dhe%2Bwalked%2Bby%2Bnight&if=false&ts=1731680195604&sw=1920&sh=1080&v=2.9.177&r=stable&ec=0&o=4126&fbp=fb.1.1731515838756.403053033568355184&ler=empty&cdl=API_unavailable&it=1731680195412&coo=false&rqm=GET
:scheme:	https
Accept:	image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding:	gzip, deflate, br, zstd
Accept-Language:	en-US,en;q=0.9
Cookie:	datr=3zfjZq1l9AGvDjz5YpPCLRgM; sb=_yLsZIXFZC2bAqYUjc46_nVS; ps_n=1; c_user=[redacted]; ar_debug=1; xs=217%3Aq_ZnuQCu5xi8zA%3A2%3A1727359909%3A-1%3A3053%3A%3AAcWSglz4vG4GjzSOI8-SOIdDgboG16pQvICQrUAgBg; fr=1d6e8jaaE9zVltRCH.AWX5gVwFsQIGl2gL0dFfCnuCls8.BnM6Fg..AAA.0.0.BnM6Gy.AWVZyDGyHs8; usida=eyJ2ZXliOjEsImlkIjoiQXNtdXA5YWpjbjJjMSIsInRpbWUiOjE3MzE0Mzc4MjN9
Priority:	i
Referer:	https://kinolorber.com/
Sec-Ch-Ua:	"Chromium";v="130", "Google Chrome";v="130", "Not?A_Brand";v="99"
Sec-Ch-Ua-Mobile:	?0
Sec-Ch-Ua-Platform:	"Windows"
Sec-Fetch-Dest:	image
Sec-Fetch-Mode:	no-cors
Sec-Fetch-Site:	cross-site
User-Agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36

Figure 9 – c_user Cookie included in URL parameters disclosed to Facebook through PageView Pixel Event on the Website



Headers Payload Preview Response Initiator Timing Cookies

▼ General

Request URL:	https://www.facebook.com/tr/?id=190239228521074&ev=SubscribedButtonClick&dl=https%3A%2F%2Fkinolorber.com%2Fproduct%2Fhe-walked-by-night-special-edition&rl=https%3A%2F%2Fkinolorber.com%2Fsearch%3Fq%3Dhe%2Bwalked%2Bby%2Bnight&if=false&ts=1731680456353&cd[buttonFeatures]=%7B%22classList%22%3A%22btn%20btn-ecommerce-primary%20btn-ecommerce-cta%20btn--cms-default%20btn-square%20%20%22%2C%22destination%22%3A%22https%3A%2F%2Fkinolorber.com%2Fcart%2Fadd%22%2C%22id%22%3A%22%22%2C%22imageUrl%22%3A%22%22%2C%22innerText%22%3A%22Add%20to%20Cart%22%2C%22numChildButtons%22%3A0%2C%22tag%22%3A%22button%22%2C%22type%22%3A%22submit%22%2C%22name%22%3A%22%22%2C%22value%22%3A%22%22%7D&cd[buttonText]=Add%20to%20Cart&cd[formFeatures]=%5B%7B%22id%22%3A%22%22%2C%22name%22%3A%22variant_id%22%2C%22tag%22%3A%22input%22%2C%22inputType%22%3A%22hidden%22%7D%5D&cd[pageFeatures]=%7B%22title%22%3A%22He%20Walked%20By%20Night%20(Blu-ray)%20-%20Kino%20Lorber%20Home%20Video%22%7D&sw=1920&sh=1080&v=2.9.177&r=stable&ec=1&o=4126&fbp=fb.1.1731515838756.403053033568355184&ler=empty&cdl=API_unavailable&it=1731680195412&coo=false&es=automatic&tm=3&rqm=GET
Request Method:	GET
Status Code:	200 OK
Remote Address:	31.13.93.35:443
Referrer Policy:	strict-origin-when-cross-origin

Figure 10 – Video Title included in URL parameters disclosed to Facebook through SubscribedButtonClick Pixel Event on the Website

116. Defendant also transmits Consumers' PII to Facebook in the form of an unencrypted and unique UID contained in the c_user cookie included in the HTTP Request Header, which can be used to find a user's personal Facebook page, as discussed in Section B(1)(a) above.

117. The information contained within the c_user cookie is considered PII because it contains "the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching behavior."[52] Because the UID can simply and easily be appended to "www.facebook.com/" to navigate to the relevant user's profile, it requires no special skill or expertise to identify the user associated with the Facebook ID, and courts have regularly upheld its status as PII.[53]

b. The Pixel Shares Consumers' Search Terms

118. In addition to capturing and sharing Consumers' PII (in violation of the VPPA) and irrespective of how the Consumer reached the web watching page, the Pixel also intercepted and shared search terms entered by Plaintiffs.

119. For example, a search for "He Walked By Night" on the Website and the resulting Pixel transmission are depicted in *Figures 1* through *Figure 3* above.

120. Such search terms, while independently confidential, may also include the capturing and sharing of searches associated with Consumers' video watching history, resulting in violation of the VPPA.

121. Plaintiffs were unaware of the interception of their confidential communications with the Website.

---

[52] *In re Nickelodeon Consumer Privacy Litigation,* 827 F.3d 262, 290 (3d Cir. 2016).
[53] *See Lebakken v. WebMD, LLC* 2022 U.S. Dist. LEXIS 201010, at *11-12 (N.D. Ga. Nov. 4, 2022); *Czarnionka v. Epoch Times Ass'n*, 2022 U.S. Dist. LEXIS 209067, at *8-10 (S.D.N.Y. Nov. 17, 2022); *Ambrose v. Boston Globe Media Partners, LLC*, 2022 U.S. Dist. LEXIS 168403, at *5-6 (D. Mass. Sept. 19, 2022).

122. Plaintiffs reasonably believed that communications to the Website were made in confidence.

123. With no notice or warning as to who was intercepting and decoding the contents of their communications, Plaintiffs were not provided notice of or given an opportunity to provide consent to the Tracking Entities' interceptions of Plaintiffs' search terms.

c. Defendant Was Told the Pixel Discloses Consumers' Data; It Knew Precisely What the Pixel Would Collect and Share

124. When a business applies with Facebook to use the Pixel, it is provided with detail about its functionality (site policy), including with respect to PII.[54]

125. To make use of the Pixel, Defendant agreed to Facebook's Business Tool Terms (the "Business Terms").

126. The Business Terms informs website owners using Facebook's tracking tools that the employment of the Pixel will result in data sharing, including with Facebook, through the automatic sharing of Pixel Event information ("Event Data") and contact information ("Contact Information").[55]

127. The Business Terms are transparent that Meta will use the Event Data and Contact Information will be processed "solely to match the Contact Information against user IDs ("Matched User IDs"), as well as to combine those user IDs with corresponding Event Data."[56]

---

[54] *See Get Started*, FACEBOOK, https://developers.facebook.com/docs/meta-pixel/get-started (last visited Nov. 15, 2024) (The Pixel "relies on Facebook cookies, which enable us to match your website visitors to their respective Facebook User accounts. Once matched, we can their actions in the Facebook Ads Manager so you can use the data . . . By default, the Pixel will track URLs visited [and] domains visited . . . .").

[55] *Meta Business Tools Terms*, FACEBOOK https://www.facebook.com/legal/terms/businesstools?paipv=0&eav=AfakosFmNyhZJOrkCsGodnMzth_uq6s403DsPEkeiKEyrj7rKyf5_t2I8wFEEUZUJlI&_rdr (last visited Nov. 15, 2024).

[56] *Id.*

128. Facebook directs parties implementing the Pixel – here, Defendant – to encrypt request information[57] *before* data can be shared.[58]

129. Facebook further provides Pixel users, such as Defendant, guidance on responsible data handling, and details how data is acquired, used, and stored, including which information is shared with Facebook.

130. Facebook educates or reminds Pixel users of their responsibility to inform their Consumers of their website's data sharing, and specifically guides website owners to obtain the requisite rights, permissions, or consents, before sharing information with any third-party.[59]

131. As a sophisticated party entering into a business arrangement with another sophisticated party, Defendant was on notice of the potential privacy violations that would result from use of the Pixel, and ignored Facebook's warnings to safely handle its Consumers' data and to warn its subscribers that the Website would disclose information in a manner that threatened Consumers' VPPA-protected PII.

3. Defendant Implemented Google's Tracking Tools on the Website

132. Google has an array of advertising products, each serving a specific function in advertising portfolios.

a. Google Ads

133. One product, Google Ads (formerly AdWords), is an advertising platform developed by Google, that allows advertisers to place bids to display advertisements, service offerings, product listings, or videos to web users.[60]

---

[57] This contrasts with Facebook's JavaScript Pixel, which automatically encrypts the data being sent. Defendant has specifically chosen the Pixel method which makes users' information visible. *See id.*

[58] *Id.*

[59] *Meta Business Help Center: Best practices for privacy and data use for Meta Business Tools*, FACEBOOK, https://www.facebook.com/business/help/363303621411154?id=818859032317965 (last visited Nov. 15, 2024).

[60] *Achieve all your goals in one place*, GOOGLE ADS, https://ads.google.com/home/goals/ (last visited Nov. 15, 2024).

134. The process advertisers using Google Ads to display ads within text-based search results is as follows: (i) advertisers create text-based ads with a title, description, and a link to the website to place within the Google search results; (ii) advertisers then choose keywords, usually related to their business or target audience, intended to trigger their ads to appear within the user's search results;[61] (iii) Google then allows advertisers to bid on those various keywords;[62] (iv) the advertiser with the highest bid wins the auction, and the ad is displayed on the search results page; and (v) the winning ad appears above or below the organic search results and is marked as an ad.

135. Google AdSense, works in conjunction with the Google Ads bidding system, allowing website owners to show Google Ads on websites and earn a revenue share from each ad each time it is viewed or clicked on their own sites.[63] The search terms that various entities bid for through Google Ads are then used by websites owners using Google AdSense to allow website owners to share in the profit Google generates from the advertising.

136. AdSense for content or AdSense for search are methods by which AdSense functions.[64] In either case, AdSense allows the website host to match ads to the website users based on the website's content and visitors.

137. Google Ads intercepted Plaintiffs' search terms, as depicted below:

[61] *Reach the right people with Search Ads*, GOOGLE ADS, https://ads.google.com/home/campaigns/search-ads/ (last visited Nov. 15, 2024).
[62] *Id*.
[63] *Home*, GOOGLE ADSENSE, https://www.google.com/adsense/start/how-it-works/ (last visited Nov. 15, 2024).
[64] *AdSense revenue share*, GOOGLE ADSENSE REVENUE, https://support.google.com/adsense/answer/180195?hl=en (last visited Nov. 15, 2024).

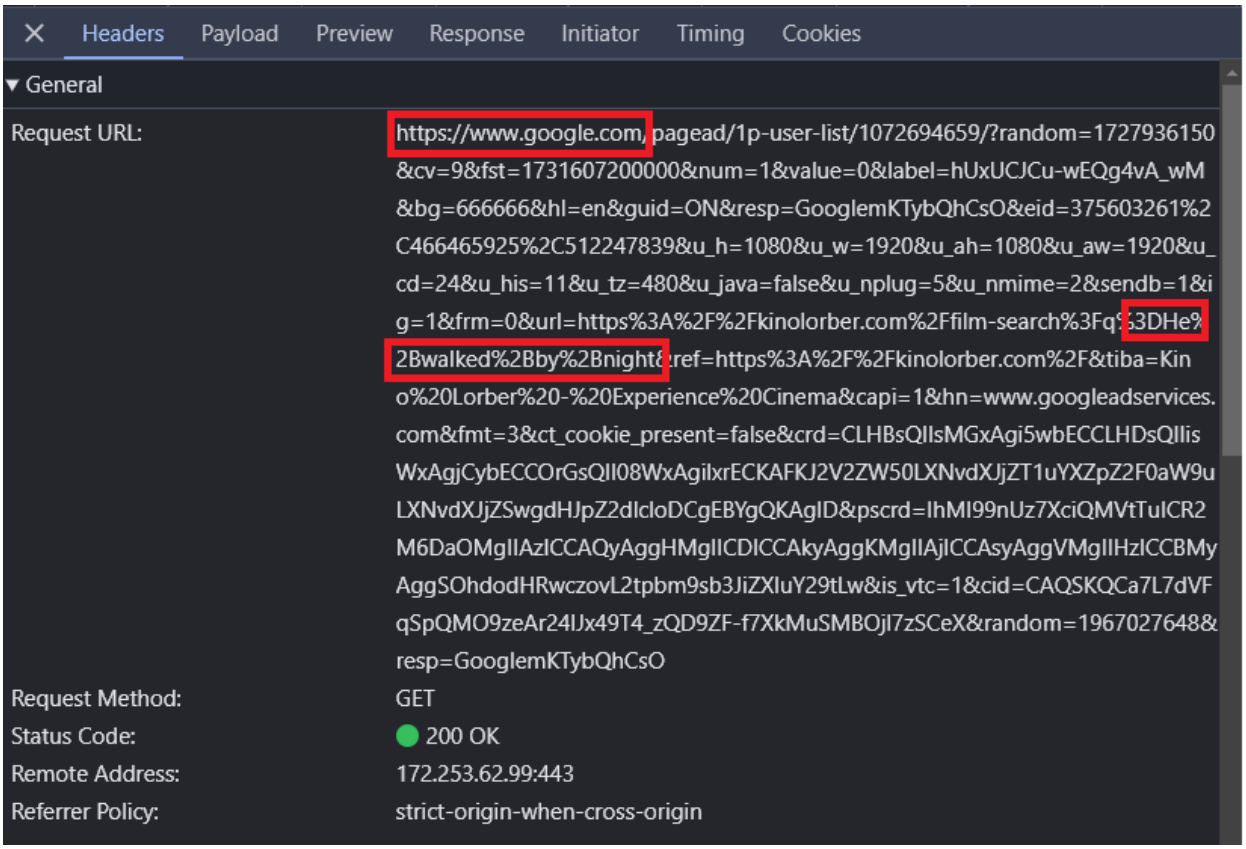


Figure 12 – Test search made on the Website resulted in Request sharing Search Terms "He Walked by Night" with Google Page Ads

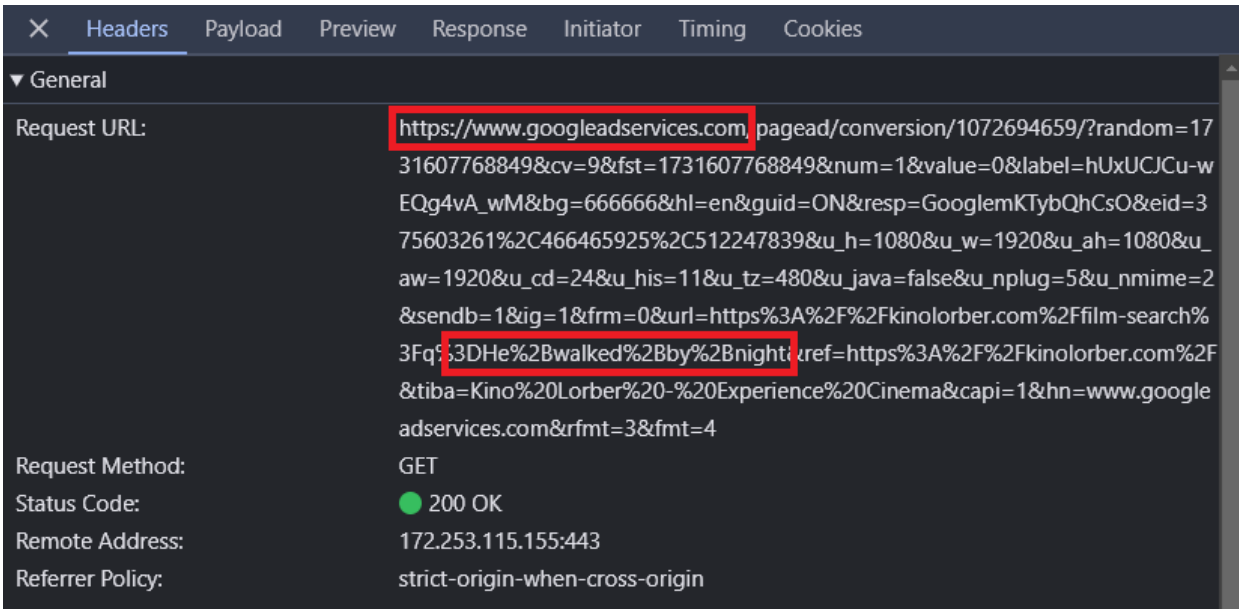


Figure 53 – Test search made on the Website resulted in Google Analytics intercepting and redirecting search terms "he walked by night" with Google

138. Google benefits when website owners utilize Google Ads and Google AdSense in connection with their websites.

139. Through Google AdSense, Google derives benefits from the ability to aggregate the search data it collects from website users to improve its own services and provide more relevant search results. By understanding patterns and trends in user behavior, Google better understands and gains unencumbered insight into what users are searching for and what they are interested in, which helps Google improve its own services, develop new products and overall increase revenues.

140. Google's collection and analysis of search results also allows it to improve its machine learning algorithms.[65] Google uses data on how users interact with search results to train its algorithms to provide more accurate and relevant search results.[66] For example, if a user clicks on a particular search result and spends more time on that page, Google learns that this page is likely more relevant to that search query. By gathering this vast array of data on all users, Google can build an advertising portfolio for each user which includes their gender, age, job industry, and interests.[67]

141. Google profits in several ways from the Website's use of the Google search engine: (i) advertisers bid and pay Google for the keywords that will result in their ads showing in search results; (ii) through AdSense search, every time a user clicks or views an ad (depending on their chosen method), the advertiser will pay Google for that click or view; (iii) and Google's ability to aggregate user search data allows them to further tailor their own products to advertisers and users alike by training its algorithms with vast amounts of search data.

[65] Elle Poole Sidell, *What Does Google Do With Your Data?*, AVAST (Dec. 18, 2020), https://www.avast.com/c-how-google-uses-your-data (last visited November 18, 2024).
[66] *Id.*
[67] *Id.*

b. Google Analytics

142. Like the Facebook Pixel, Google Analytics ("GA") collect data about user interactions with a website, including: link clicks, button clicks, form submissions, conversions, shopping cart abandonment, adding items to carts, removing items from carts, file downloads, scrolling behavior, video views, call to action performance, table of contents clicks, and other customizable events.[68]

143. The data collected through GA is sent back to Google, which associates the activity with the website it was collected from.[69] Notably, Google notifies web developers that developers should provide "users with clear and comprehensive information about the data . . . collect[ed] on [their] websites" and to obtain "consent for that collection where legally required."[70]

144. In short, the use of GA represents specific data collection practices and settings and pre-determined destinations for that data. Google itself is aware of the potential legal violations its data collection tools are capable of, and puts the onus of warning users onto the website developers, such as Defendant.

145. Here, Defendant added GA to its Website, which resulted in the interception by and redirection of Plaintiffs' search terms to Google, as depicted from the example taken directly from the Website below:

[68] Zach Paruch, *What Is Google Tag Manager & How Does It Work?*, SEMRUSH: BLOG (Jan. 4, 2024) https://www.semrush.com/blog/beginners-guide-to-google-tag-manager/ (last visited November 18, 2024).
[69] *Tag Manager Help: About the Google Tag*, GOOGLE, https://support.google.com/tagmanager/answer/11994839?hl=en (last visited November 18, 2024).
[70] *Id.*

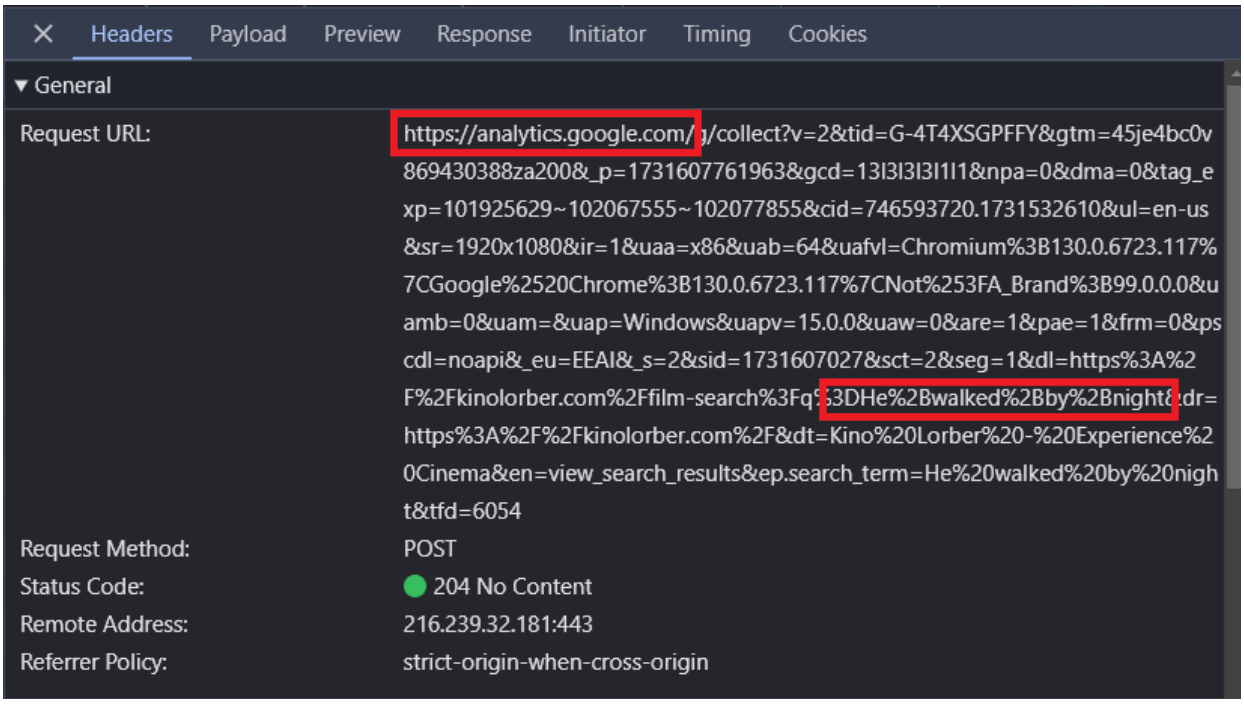


Figure 14 – Test search made on the Website resulted in Google Analytics intercepting and redirecting search terms "he walked by night" with Google

146. After arriving at those common destinations, the Google products provide analysis and feedback which help the Defendant to monetize the collected information as discussed above in paragraphs 130 through 138.

4. Defendant Implemented TTD's Tracking Tools On The Website

147. The Trade Desk is a demand-side platform ("DSP") – meaning that the Trade Desk provides automation software to help advertisers buy advertisements.[71] The Trade Desk provides advertisement purchasers with tools to manage and optimize their digital advertising campaigns across various channels and inventory sources.[72] As a DSP, the Trade Desk works with Supply Side platforms ("SSPs"), which are sell-side platforms used to manage the supply of ad inventories for publishers or those with advertising space on their website to sell.[73] The Trade

[71] *What is a demand-side platform (DSP)*, ADJUST, https://www.adjust.com/glossary/demand-side-platform/ (last visited Nov. 15, 2024).
[72] *Trackers: The Trade Desk (adsrvr.org)*, BETTER, https://better.fyi/trackers/adsrvr.org/ (last visited Nov. 15, 2024)
[73] *What is a Supply-Side Platform?*, PUBLIFT, https://www.publift.com/adteach/what-is-a-supply-side-platform (last visited Nov. 15, 2024).

Desk is integrated with many SSPs that rely on the advertising spend generated from The Trade Desk's advertisers.[74]

148. The Trade Desk offers a range of technologies, products, and services that it touts as tailored to personalize the delivery of digital content to individual users.[75] As for Trade Desk's personalized advertisements to users, CEO Jeff Green described Trade Desk's Unified ID 2.0 marketing technology: "We will have effectively solved the identity matching challenge of the entire open internet on a scale well beyond anything cookies have ever accomplished, and all while providing consumers with much greater control over their privacy."[76]

149. Among the tracking technologies offered by the Trade Desk, employed by the Website, for the purposes of tracking user behavior and gathering data to enable targeted advertising, is the Trade Desk Universal Pixel ("TTD Pixel").[77] Similar to the Facebook Pixel, the TTD Pixel is enabled by placing the TTD Pixel code within the website's code, which enables the capture of data on every page of the website and across multiple websites.[78] The TTD Pixel operates to enhance the effectiveness of programmatic advertising campaigns by giving marketers insight into user data.[79]

150. The TTD Pixel, like other pixels, is a tracking tool that can be integrated with the Trade Desk's platform (the "Platform").[80] The TTD Pixel is a technology that allows advertisers

---

[74] *Id*.

[75] *News Details: The Trade Desk Reports Fourth Quarter and Fiscal Year 2022 Financial Results; Announces $700 Million Share Repurchase Program*, THETRADEDESK: INVESTOR RELATIONS (Feb. 15, 2023), https://investors.thetradedesk.com/news-events/news-details/2023/The-Trade-Desk-Reports-Fourth-Quarter-and-Fiscal-Year-2022-Financial-Results-Announces-700-Million-Share-Repurchase-Program/default.aspx#:~:text=2022%20revenue%20increased%2032%25%20year%20over%20year%20to%20%241%2C578%20million (last visited November 18, 2024).

[76] Chris Kelly, *Trade Desk revenue up 24% as advertisers continue shift to CTV, retail media*, MARKETINGDIVE (Feb. 15, 2023), https://www.marketingdive.com/news/trade-desk-earnings-q4-ctv-retail-media/642825/ (last visited November 18, 2024).

[77] *See Tracking Tags,* THE TRADE DESK, *https://partner.thetradedesk.com/v3/portal/data/doc/TrackingTagsOverview* (last visited Nov.15, 2024.

[78] *Universal Pixel*, LOCKHEED MARTIN, https://www.lockheedmartin.com/content/dam/lockheed-martin/eo/documents/contact/TTD_UniversalPixel_Overview.pdf (last visited Nov. 15, 2024).

[79] Klaudia Smykowska, *How to Prove the Value of Upper-Funnel Display Advertising, RISE* https://www.meetrise.com/blog/prove-value-of-upper-funnel-display-advertising (last visited Nov. 15, 2024).

[80] The Trade Desk platform refers to the Trade Desk's self-service technologies for buying and managing digital advertising campaigns across various channels and formats (the "Platform"). The Platform allows advertisers to use

and site operators a way to "spend less time placing tags, gain more visibility into user data, and analyze reporting at a more granular level . . . all with the placement of a single tag."[81] The TTD Pixel collects information such as demographics, browsing behavior, and conversion events: the exact information collected in our case will be discussed below.[82] The TTD Pixel is not limited to computer or browser-based browsing, it is capable of collecting information from mobile platforms, including how a user interacts with mobile applications and specific details regarding the mobile device being used to access the content and the applications.[83]

151. An advertiser or website operator that uses the Platform to run their campaigns can leverage the TTD Pixel tracking capabilities to collect data on how users interact across various websites, mobile applications, television, and other technologies.[84] The TTD Pixel competes with other advertising and tracking technologies such as DoubleClick by Google, Facebook Ads, and Scorecard.

a. The Trade Desk benefits from the Website's use of the TTD Pixel

152. Integration of the TTD Pixel by the Defendant provides numerous benefits to Trade Desk and Defendant, as discussed below.

153. The first benefit provided by the TTD Pixel to the Trade Desk is the data collection itself. This data collection allows the Trade Desk to segment user information to create target audiences and track conversions enabling them to offer advertisers the best possible ad placement

---

data to better target specific audiences using the TTD Pixel, along with other technologies. The Platform also provides real-time bidding, where advertisers bid on ad impressions, and can access insights into impressions, clicks, conversions, and audience engagement metrics. The Platform allows for cross-device advertising to smartphones, tablets, TVs, and desktop computers. Overall, the Platform provides advertisers with advertising capabilities, audience targeting, real-time bidding, data analytics, and control over their digital ad campaigns.

[81] *Universal Pixel*, LOCKHEED MARTIN, https://www.lockheedmartin.com/content/dam/lockheed-martin/eo/documents/contact/TTD_UniversalPixel_Overview.pdf (last visited Nov. 15, 2024).

[82] *See Tracking Tags,* THE TRADE DESK, *https://partner.thetradedesk.com/v3/portal/data/doc/TrackingTagsOverview* (last visited Nov.15, 2024.

[83] *Privacy and The Trade Desk Platform*, THETRADEDESK (Nov. 5, 2024), https://www.thetradedesk.com/us/privacy (last visited November 18, 2024).

[84] *Id*.

for their websites and use of their money.[85] For example, the TTD Pixel tracking enables the Trade Desk to collect user data utilizing the TTD Pixel allowing the tacking of user's demographic information, browsing behaviors, preferences, and interactions with websites.[86] This data is then sent to an SSP who analyzes the bids from multiple DSPs, such as the Trade Desk, and enables the user to be targeted more effectively based on their information.[87] Essentially then, the Trade Desk is reliant on this information for its business to remain viable.

154. The TTD Pixel also allows the Trade Desk to retarget users by creating lookalike audiences because the TTD Pixel is "essentially [] just storing a group of people and information about them."[88] A lookalike audience is a group of people who are likely to be interested in a business because they're similar to existing customers.[89] With the lookalike audiences developed, the Trade Desk can bid on for advertising space for advertisers from SSPs that are targeting a similar demographic with more confidence that those website users will get clicks or conversions.[90]

155. Finally, given Trade Desk's main business is charging their clients or ad publishers a certain percentage of the gross spending on the Trade Desk platform, increasing the effectiveness of their ad campaign leads to increased revenues. This is because with the increased effectiveness of Trade Desk's advertising targeting by improving advertising conversion rates

---

[85] Erin Jeffery, *What are Pixels and Why Do I Need to Use Them?*, AX INSIGHTS (Sept. 3, 2020), https://audiencex.com/insights/what-are-pixels-and-why-do-i-need-to-use-them/ (last visited November 18, 2024).

[86] Andy Pitre, *Ad Tracking: What It Is & How to Do It*, HUBSPOT: BLOG (March 10, 2022), https://blog.hubspot.com/blog/tabid/6307/bid/7249/a-marketer-s-guide-to-tracking-online-campaigns.aspx (last visited November 18, 2024).

[87] *Programmatic Advertising: Your Guide to DMPs, DSPs, and SSPs*, GROWTH MARKETING GENIE, https://growthmarketinggenie.com/blog/programmatic-advertising-dmps-dsps-ssps/ (last visited Nov. 15, 2024).

[88] Erin Jeffery, *What are Pixels and Why Do I Need to Use Them?*, AX INSIGHTS (Sept. 3, 2020), https://audiencex.com/insights/what-are-pixels-and-why-do-i-need-to-use-them/ (last visited November 18, 2024).

[89] *Use Lookalike segments to grow your audience*, GOOGLE ADS HELP, https://support.google.com/google-ads/answer/13541369?hl=en#:~:text=Lookalike%20segments%20are%20groups%20of,and%20app%2C%20or%20YouTube%20channel. (last visited Nov. 15, 2024).

[90] *Id*.

(the rate at which clicks turn to sales),[91] other advertisers will shift their business to Trade Desk, further increasing Trade Desk revenue derived from ad sales. [92]

156. On the Website, the TTD Pixel intercepts the Search Terms after they are entered into the search bar and before the results of the search are received and loaded onto the user's device, as depicted below:

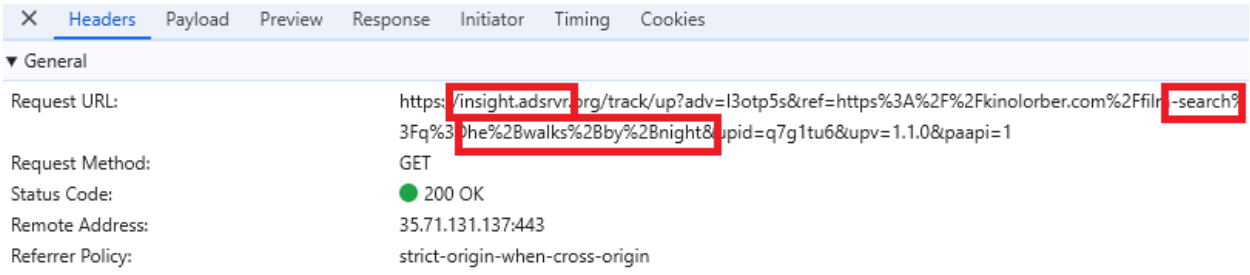


Figure 65 - Inputting Search Terms into Search Bar results in TTD Pixel Intercepting the Search Terms

b. Defendant Benefits from the Website's use of the TTD Pixel

157. The main benefit to the Defendant is the ability to sell advertising space on the Website or purchase advertising to target users more effectively. Utilizing the TTD Pixel provides the Defendant a way to optimize their ad space on the Website by only showing ads relevant to their users, based on the information shared through the TTD Pixel.[93] This ensures that ad space on the Website is not wasted, and both the Website and Defendant respectively realize more revenue from the user clicks that turn into conversions based on their revenue sharing agreements.

158. Next, Defendant benefits in the form of time savings in that they no longer need to seek out ad publishers. Traditionally, buying ads required manual negotiation between the

[91] *What is a conversion rate?*, ADJUST, https://www.adjust.com/glossary/conversion-rate/ (last visited Nov. 15, 2024).
[92] Trevor Jennewine, *How Does The Trade Desk Make Money?*, THE MOTLEY FOOL (Oct. 27, 2021), https://www.nasdaq.com/articles/how-does-the-trade-desk-make-money-2021-10-27 (last visited Nov. 18, 2023).
[93] Andy Pitre, *Ad Tracking: What It Is & How to Do It*, HUBSPOT: BLOG (March 10, 2022), https://blog.hubspot.com/blog/tabid/6307/bid/7249/a-marketer-s-guide-to-tracking-online-campaigns.aspx (last visited Nov. 18, 2024).

buyer of an ad and the website host.[94] Now, with the automated marketing enabled by the Trade Desk and TTD Pixel, Defendant can place the TTD Pixel on their Website and give their user and advertising space information to the Trade Desk – the rest of the process is completely automated.

159. Furthermore, by tracking user behavior across the Website, Defendant can determine which users to advertise to, allowing the Website to derive further revenue. [95] The Website tracks user behavior across various pages of its website, which enables Defendant to add certain elements or buttons to their website that increase users' exposure to ads.[96]

C. Plaintiffs Did Not Consent to Defendant's Sharing of Plaintiffs' Search Terms

160. Plaintiffs were unaware of the Pixel's, and other Tracking Tools', interception of their confidential communications with the Website. The absent class members were equally unaware of the Tracking Tools intercepting their confidential communications with the Website.

161. Plaintiffs reasonably believed that communications to the Website were made in confidence. Absent class members held the same expectation in connection with their own communications between themselves and the Website.

162. With no notice or warning as to who was intercepting and decoding the contents of their communications, Plaintiffs were not provided notice of or given an opportunity to provide consent to The Trade Desk's and other Tracking Tools' interceptions of Plaintiffs' search terms.

163. Meta and Google, by way of example, guide and caution website operators of the dangers of using their tracking tools without first providing notice of and then obtaining valid consent for invasively collecting consumers' protected data and either making that data available

---

[94] Trevor Jennewine, *How Does The Trade Desk Make Money?*, THE MOTLEY FOOL (Oct. 27, 2021), https://www.nasdaq.com/articles/how-does-the-trade-desk-make-money-2021-10-27 (last visited Nov. 18, 2024).
[95] *Id*.
[96] Erin Jeffery, *What are Pixels and Why Do I Need to Use Them?*, AX INSIGHTS (Sept. 3, 2020), https://audiencex.com/insights/what-are-pixels-and-why-do-i-need-to-use-them/ (last visited Nov. 18, 2024).

to third-parties or allowing third parties to intercept consumers' protected information. Defendant agreed to these terms, in order to utilize and employ the Tracking Tools.

164. In contravention to Meta's and Google's terms and guidance, Plaintiffs were not given notice of the use of the Tracking Tools on the Website.

165. As a result, Plaintiffs did not and could not provide consent to the collection and sharing of their data when visiting the Website, running searches on the Website, and purchasing films from the Website.

D. Plaintiffs Have a Privacy Right in their Search Terms

166. As Senator Leahy aptly foresaw, the time has come where companies can easily build profiles of customers based on their consumer habits.

167. Communications shared between consumers and companies appear to be private but, in reality, the contents of those messages are regularly shared.

168. Here, Defendant shares consumers' information, including search terms, with the Tracking Entities.

169. Search terms are inherently private. This is particularly true when the searches are communicated in confidence, or presumed to be private. All search terms are personal in nature, but there is an obviously heightened want for the searches to be kept confidential when the search terms themselves contain private information.

170. As described in Section A(1), descriptions and summaries of requested pre-recorded audio visual materials are private information worthy of federal protection.

171. Users search for video materials on the Website using search terms. The search terms, when associated with descriptions or summaries of the pre-recorded videos, pertain to more than users' basic privacy.

172. This private information is then shared with various advertising services, including the Tracking Entities.

D. The Website Does Not Obtain Consumers' Informed, Written Consent Pursuant to the VPPA.

173. The Website does not seek nor obtain permission from Consumers, including Plaintiffs and the Class, to share the Consumers' PII with third parties, including Facebook.

174. The sign-up process for Kino Lorber does not seek or obtain informed, written consent.

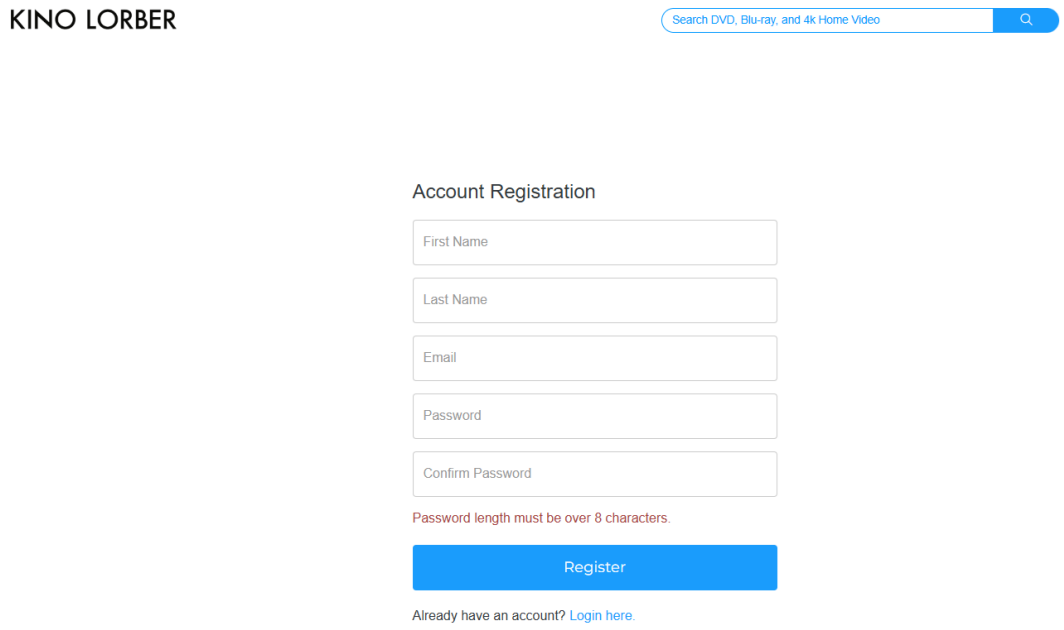


Figure 16 – The Website's Account Registration Webpage

175. To the extent information about any of the Website's data sharing can be located, the language is not (i) presented to consumers of the site in a transparent manner, or where it must be viewed by visitors to the website; (ii) made available as part of the sign-up process; (iii) offered to consumers as checkbox or e-signature field, or as any form of consent; and (iv) presented in

terms that sufficiently warn Consumers that their information, protected by the VPPA, will be shared with third parties.[97]

TOLLING

176. The statutes of limitations applicable to Plaintiffs' and the Class's claims were tolled by Defendant's conduct and Plaintiffs' and Class Members' delayed discovery of their claims.

177. As alleged above, Plaintiffs and members of the Class did not know and could not have known when they used the Website that Defendant was disclosing their information and communications to third parties. Plaintiffs and members of the Class could not have discovered Defendant's unlawful conduct with reasonable diligence.

178. Defendant secretly incorporated the Facebook Pixel into the Website, providing no indication to consumers that their communications would be disclosed to these third parties.

179. Defendant had exclusive and superior knowledge that the Tracking Entities' tracking tools incorporated on its Website would disclose consumers' protected and private information and confidential communications, yet failed to disclose that by interacting with the Website, Plaintiffs' and Class members' PII would be disclosed to third parties.

180. Plaintiffs and members of the Class could not with due diligence have discovered the full scope of Defendant's conduct because the incorporation of the tracking entities' tracking tools is highly technical and there were no disclosures or other indication that would inform a reasonable consumer or Website user that Defendant was disclosing and allowing the interception of such information to these third parties.

181. The earliest Plaintiffs and Class members could have known about Defendant's conduct was in connection with their investigation and the work done on their behalf in preparation of filing of this Complaint.

[97] *See Privacy Policy*, Kino Lorber, https://kinolorber.com/privacy-policy (last visited Nov. 18, 2024).

CLASS ACTION ALLEGATIONS

182. Plaintiffs bring this action individually and on behalf of the following Class:

> All persons in the United States with an account with the Website that had their Personally Identifiable Information improperly disclosed to third parties through the use of the Tracking Tools (the "Class").

183. Plaintiff Padow brings this action individual and on behalf of the following Class:

> All persons in California with an account with the Website that had their Personally Identifiable Information improperly disclosed to third parties through the use of the Tracking Tools (the "California Class").

184. Specifically excluded from the Classes are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendant, and their heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

185. Plaintiffs reserve the right to amend the Class definitions above if further investigation and/or discovery reveals that the Classes should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

186. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

187. Numerosity (Rule 23(a)(1)): At this time, Plaintiffs do not know the exact number of members of the aforementioned Class. However, given the popularity of Defendant's Website, the numbers of persons within the Classes are believed to be so numerous that joinder of all members is impractical.

188. Typicality of Claims (Rule 23(a)(3)): Plaintiffs' claims are typical of those of the Class because Plaintiffs, like all members of the Classes, purchased from, and used, the Website

to search for videos, and had their PII, search terms, metadata, and detailed URLs, collected and disclosed by Defendant's use of the Tracking Tools.

189. Adequacy of Representation (Rule 23(a)(4)): Plaintiffs will fairly and adequately represent and protect the interests of the Classes. Plaintiffs have no interests antagonistic to, nor in conflict with, the Class or the California Class. Plaintiffs have retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

190. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class members is relatively small, the expense and burden of individual litigation make it impossible for individual Class members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue their wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

191. Commonality and Predominance (Rule 23(a)(2), 23(b)(3)): There is a well-defined community of interest in the questions of law and fact involved in this case. Questions of law and fact common to the members of the Class that predominate over questions that may affect individual members of the Class include:

a. Whether Defendant collected Plaintiffs' and the Class's PII;

b. Whether Defendant unlawfully disclosed and continue to disclose the PII of consumers of the Website in violation of the VPPA;

c. Whether Defendant's disclosures were committed knowingly; and

d. Whether Defendant disclosed Plaintiffs' and the Class's PII, search terms, and browsing history without consent.

192. Information concerning Defendant's Website's data sharing practices and account members is available from Defendant's or third-party records.

193. Plaintiffs know of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

194. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

195. Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

196. Given that Defendant's conduct is ongoing, monetary damages are insufficient and there is no complete and adequate remedy at law.

COUNT I

VIOLATION OF THE VIDEO PRIVACY PROTECTION ACT
18 U.S.C. § 2710, *et seq*.
(On Behalf of Plaintiffs and the Class)

197. Plaintiffs hereby incorporate by reference and re-allege each and every allegation set forth above in in all preceding paragraphs of this Complaint.

198. Plaintiffs bring this count on behalf of themselves and all members of the Class.

199. The VPPA provides that "a video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer shall be liable to the aggrieved person for the relief provided in subsection (d)." 18 U.S.C. § 2710(b)(1).

200. "Personally-identifiable information" is defined to include "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3).

201. A "video tape service provider" is "any person, engaged in the business, in or affecting interstate commerce, of rental, sale, or delivery of pre-recorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710(a)(4).

202. Defendant violated this statute by knowingly disclosing Plaintiffs' and other Class Members' personally identifiable information to Facebook.

203. Defendant, through the Website, engage in the business of selling video content to consumers, including Plaintiffs and the other Class Members, and other users. The Website sells videos to consumers, including Plaintiffs and the other Class Members, by making those materials available to Plaintiffs and the other Class Members on the Website for purchase.

204. Defendant is a "video tape service provider" because it curates, provides access to, and causes the delivery of thousands of videos on the Website, thereby "engag[ing] in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710(a)(4).

205. Defendant solicits individuals to pay to obtain films from the Website.

206. Plaintiffs and members of the Class are "consumers" because they paid to purchase audio-visual materials from Defendant's Website. 18 U.S.C. § 2710(a)(1).

207. Plaintiffs and members of the Class purchased videos on the Website.

208. Defendant disclosed Plaintiffs' and Class Members' personally identifiable information to Facebook. Defendant utilized the Pixel which forced Plaintiffs' web browser to transmit Plaintiffs' identifying information, like their Facebook ID, along with Plaintiffs' and Class Members' event data, including the title of the videos they viewed, to Facebook.

209. Defendant knowingly disclosed Plaintiffs' and Class Members' PII, which is triggered automatically through Defendant's use of the Pixel. No additional steps on the part of the Defendant, Facebook, or any third-party are required. Once the Pixel's routine exchange of

information is complete, the UID that becomes available can be used by any individual to easily identify a Facebook user. *See* Section B(1)(a) (process to identify individual using UID).

210. Plaintiffs and members of the Class did not provide Defendant with any form of consent—either written or otherwise—to disclose their PII to Facebook. Defendant failed to obtain "informed, written consent" from consumers – including Plaintiffs and members of the Class – "in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer" and "at the election of the consumer," either "given at the time the disclosure is sought" or "given in advance for a set period of time, not to exceed 2 years or until consent is withdrawn by the consumer, whichever is sooner." 18 U.S.C. § 2710(b)(2)(B)(i)-(ii).

211. Defendant's disclosures of Plaintiffs' and Class Members' PII were not made in the "ordinary course of business" as the term is defined by the VPPA. In particular, Defendant's disclosures to Facebook were not necessary for "debt collection activities, order fulfillment, request processing, [or] transfer of ownership." 18 U.S.C. § 2710(a)(2). Instead, Plaintiffs' and Class Members' PII was used for improving marketing effectiveness.

212. In addition, the VPPA creates an opt-out right for consumers in 18 U.S.C. § 2710(2)(B)(iii). It requires video tape service providers to also "provide[] an opportunity for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election." Defendant failed to provide an opportunity to opt out as required by the VPPA.

213. On behalf of themselves and the Class, Plaintiffs seek: (i) declaratory relief as to Defendant; (ii) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Defendant to comply with VPPA's requirements for protecting a consumer's PII; (iii) statutory damages of $2,500 for each violation of the VPPA pursuant to 18 U.S.C. § 2710(c); and (iv) reasonable attorneys' fees and costs and other litigation expenses.

Injunctive Relief Of Defendant's Ongoing VPPA Violations

214. An actual and immediate controversy has arisen and now exists between Plaintiffs and the putative classes they seek to represent, and Defendant, which parties have a genuine and opposing interest in and which their interests are direct and substantial. Defendant has violated, and continues to violate, Plaintiffs' and Class Members' rights to protect their PII under the VPPA.

215. Plaintiffs have demonstrated that they are likely to succeed on the merits of their claims, and are thus entitled to declaratory and injunctive relief.

216. Plaintiffs have no adequate remedy at law to stop the continuing violations of the VPPA by Defendant. Unless enjoined by the Court, Defendant will continue to infringe on the privacy rights of Plaintiffs, Class Members, and the absent Class Members, and will continue to cause, or allow to be caused, irreparable harm to Plaintiffs and Class Members. Injunctive relief is in the public interest to protect the PII of Plaintiffs and Class Members, and other consumers that would be irreparably harmed through continued disclosure of their PII.

217. Defendant completely disregards their obligation under the VPPA by loading the Pixel onto the Website and facilitating the sharing of consumers' PII with third parties for any ordinary person to access and use.

218. Despite brazenly violating the VPPA, consumers were provided with no notice of the employment of the Pixel and no indication of how or how much of their information was shared with third parties. Worse, in further violation of the VPPA, Defendant did not seek or obtain any form of consent from subscribers for the use of the Tracking Tools to share information improperly pulled from the Website.

219. This threat of injury to Plaintiffs and members of the Class from the continuous violations requires temporary, preliminary, and permanent injunctive relief to ensure their PII is protected from future disclosure.

COUNT II

VIOLATION OF THE FEDERAL WIRETAP ACT
18 U.S.C. § 2510, *et seq*.
(On Behalf of Plaintiffs and the Class)

220. Plaintiffs hereby incorporate by reference and re-allege herein the allegations contained in all preceding paragraphs of this Complaint.

221. Plaintiffs bring this claim individually and on behalf of the members of the Class against Defendant.

222. Codified under 18 U.S.C. §§ 2510 *et seq.*, the Federal Wiretap Act (the "Wiretap Act") prohibits the interception of any wire, oral, or electronic communications without the consent of at least one authorized party to the communication.

223. The Wiretap Act confers a civil private right of action to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

224. The Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

225. The Wiretap Act defines "contents" as "includ[ing] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

226. The Wiretap Act defines "person as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6).

227. The Wiretap Act defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part

by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce . . . .” 18 U.S.C. § 2510(12).

228. Defendant is a person for purposes of the Wiretap Act.

229. The Facebook Pixel and other Tracking Tools constitute a “device or apparatus which can be used to intercept a wire, oral, or electronic communication.” 18 U.S.C. § 2510(5).

230. The confidential communications Plaintiffs and members of the Class had with the Website, in the form of their search terms and browsing information, were intercepted by the Tracking Entities and such communications were “electronic communications” under 18 U.S.C. § 2510(12).

231. Plaintiffs and members of the Class had a reasonable expectation of privacy in their electronic communications with the Website in the form of their search terms submitted to the Website and browsing information. Even if Plaintiffs and members of the Class had no reasonable expectation of privacy in the electronic communications, Plaintiffs’ and Class Members’ electronic communications with the Website included descriptions and summaries of the pre-recorded video content they searched for along with their PII, giving rise to a reasonable expectation of privacy under the VPPA.

232. Plaintiffs and members of the Class reasonably expected that the Tracking Entities were not intercepting, recording, or disclosing their electronic communications with the Website.

233. Within the relevant time period, the electronic communications between Plaintiffs and members of the Class and the Website were intercepted during their transmission, without consent, and for the unlawful and wrongful purpose of monetizing their private information, which includes the purpose of using such private information to develop advertising and marketing strategies.

234. Interception of Plaintiffs’ and Class Members’ confidential communications with the Website occurs whenever a user uses the Website’s search bar, and when navigating various webpages of the Website.

235. At all times relevant to this Complaint, Defendant's conduct was knowing, willful, and intentional, as the Defendant is a sophisticated party with full knowledge regarding the functionality of the Tracking Tools, including that allowing the Tracking Tools to be implemented on the Website would cause the private communications of their users to be shared with the Tracking Entities.

236. Plaintiffs and members of the Class were never asked for their consent to share their confidential electronic communications with the Website with third parties. Indeed, such consent could not have been given as Defendant never sought any form of consent from Plaintiffs or members of Class to intercept, record, and disclose their private communications with the Website.

237. As detailed above, the Tracking Entities' unauthorized interception, disclosure and use of Plaintiffs' and the Class Members' confidential communications was only possible through Defendant's knowing, willful, or intentional placement of the Tracking Tools on the Website. 18 U.S.C. § 2511(1)(a).

238. Plaintiffs and members of the Class have been damaged due to the unauthorized interception, disclosure, and use of their confidential communications in violation of 18 U.S.C. § 2520. As such, Plaintiffs and members of the Class are entitled to: (1) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and members of the Class and any profits made by the Tracking Entities as a result of the violation, or (b) statutory damages of whichever is the greater of $100 per day per violation or $10,000; and (2) appropriate equitable or declaratory relief; (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT III

VIOLATION OF THE CALIFORNIA'S INVASION OF PRIVACY ACT
Cal. Penal Code § 631
(On Behalf of Plaintiff Padow and the California Class)

239. Plaintiff Padow hereby incorporate by reference and re-allege herein the allegations contained in all preceding paragraphs of this Complaint.

240. Plaintiff Padow brings this count on behalf of himself and all members of the California Class.

241. CIPA provides that a person is liable to another where, "by means of any machine, instrument, contrivance, or in any other manner," committed any of the following: (i) intentionally tapped, or made any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, cable, or instrument of any internal telephonic communication system; or (ii) willfully and without consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state; or (iii) uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained; or (iv) aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit or cause to be done any of the acts or things mentioned above in this section. Cal. Penal Code Section 631(a).

242. The Ninth Circuit has confirmed that one of the purposes of wiretapping statutes is to "prevent the acquisition of the contents of a message by an unauthorized third-party . . . ." *In re Facebook Internet Tracking Litig.*, 956 F.3d 589, 608 (9th Cir. 2020). In dealing specifically with CIPA, the California Supreme court has similarly concluded that the objective of CIPA is to protect a person's communications "from a situation where the other person on the other end of the line permits an outsider" to monitor the communication. *Ribas v. Clark*, 38 Cal. 3d 355, 364 (1985); *see Smith v. LoanMe*, 11 Cal. 5th 183, 200 (2021).

243. The Website, including the Tracking Tools placed upon them, is a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

244. Within the relevant time period, Plaintiff Padow and members of the California Class used the search function to communicate search terms to Defendant, with the expectation of receiving search results provided by Defendant.

245. Within the relevant time period, the Tracking Entities, without the consent of all parties to the communication, or in any unauthorized manner, willfully read or attempted to read or learn the contents or meaning of electronic communications of Plaintiff Padow and the California Class Members, contemporaneous with the communications transit through or passing over any wire, line or cable or with the communications sending from or being received at any place within California.

246. The information collected by the Tracking Tools was not for the sole benefit of the Tracking Entities.

247. Within the relevant time period, Defendant also aided, agreed with, conspired with, and employed the Tracking Entities to implement the tracking tools and to violate CIPA § 631.

248. Within the relevant time period, Defendant aided, agreed with, conspired with, and employed the Tracking Entities to accomplish the wrongful conduct at issue here.

249. Plaintiff Padow and members of the California Class did not authorize or consent to the tracking, interception, and collection of any of their electronic communications.

250. The violation of section 631 constitutes an invasion of privacy sufficient to confer Article III standing.

COUNT IV

INTRUSION UPON SECLUSION
(On Behalf of Plaintiffs and the Class)

251. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in all preceding paragraphs of this Complaint.

252. Plaintiffs bring this claim individually and on behalf of the members of the proposed Class against Defendant.

253. Defendant intentionally intruded upon Class Members' solitude or seclusion in that it effectively placed Meta in the middle of conversations including search terms, precise webpage locations, and PII to which it was not an authorized party.

254. Defendant's participation in Meta's tracking and interception of PII was not authorized by Plaintiffs or Class Members.

255. Defendant's enabling of Meta's intentional intrusion into Plaintiffs' and Class Members' internet communications including PII and their computing devices and web-browsers was highly offensive to a reasonable person in that they violated federal and state criminal and civil laws designed to protect individuals' privacy and against theft.

256. Secret monitoring of search terms, precise webpage locations, and PII is highly offensive behavior.

257. Public polling on internet tracking has consistently revealed that the overwhelming majority of Americans believe it is important or very important to be "in control of who can get information" about them; to not be tracked without their consent; and to be in "control[] of what information is collected about [them]." The desire to control one's information is only heightened while a person is handling PII. Plaintiffs and Class Members have been damaged by Defendant's facilitation of Meta's intrusion upon their seclusion and are entitled to reasonable compensation including but not limited to disgorgement of profits related to the unlawful internet tracking.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek judgment against Defendant, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiffs as the representatives of the Class and their counsel as Class Counsel;

(b) For an order declaring that Defendant's conduct violates the statutes referenced herein;

(c) For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

(d) For entry of an order for injunctive and declaratory relief as described herein, including, but not limited to requiring Defendant to immediately (i) remove the Facebook Pixel from the Website or (ii) add, and obtain, the appropriate consent from subscribers;

(e) For damages in amounts to be determined by the Court and/or jury;

(f) For an award of statutory damages or penalties to the extent available;

(g) For Defendant to pay $2,500.00 to Plaintiffs and members of the Class, as provided by the VPPA, 18 U.S.C. § 2710(c)(2)(A);

(h) For pre-judgment interest on all amounts awarded;

(i) For an order of restitution and all other forms of monetary relief;

(j) An award of all reasonable attorneys' fees and costs; and

(k) Such other and further relief as the Court deems necessary and appropriate.

DEMAND FOR TRIAL BY JURY

Plaintiffs demand a trial by jury of all issues so triable.

Dated: November 18, 2024

LEVI & KORSINSKY, LLP

By: *Mark S. Reich*

Mark S. Reich (MR-4166)
Gary S. Ishimoto*
LEVI & KORSINSKY, LLP
33 Whitehall Street, 17th Floor
New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: mreich@zlk.com
Email: gishimoto@zlk.com

Counsel for Plaintiffs

**pro hac vice* forthcoming